BY ORDER OF THE COMMANDER
UNITED STATES AIR FORCES IN
EUROPE

UNITED STATES AIR FORCES IN
EUROPE INSTRUCTION 33-283

16 SEPTEMBER 2016

Communications and Information

OPERATIONAL DOCTRINE FOR SAFEGUARDING AND CONTROL OF WEAPONS STORAGE AND SECURITY SYSTEM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is available for downloading from the e-Publishing website at **www.e-Publishing.af.mil/**

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ USAFE/A10NM

Certified by: HQ USAFE/A10N
(Col Marc Sands)

Supersedes: USAFEI 33-201, 3 July 2013

Pages: 55

This instruction implements Air Force Policy Directive (AFPD) 17-1, *Information Dominance Governance and Management*. This instruction applies to all personnel assigned to United States Air Forces in Europe (USAFE) units with a Weapons Storage and Security System (WS3) mission. It does not apply to Air National Guard (ANG) or Air Force Reserve Command (AFRC) units. It outlines the control, accounting, and handling procedures for this material. Refer technical comments or recommended changes and conflicts between this and other publications on an AF Form 847, *Recommendation for Change of Publication***,** through channels, to the Nuclear Operations Division (HQ USAFE/A10N), Unit 3050, Box 15, APO AE 09094-5015. Ensure that any local instructions or supplements are created in accordance with Air Force Instruction (AFI) 33-360, *Publications and Forms Management*. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located in AFRIMS (AF Portal). Units will contact the applicable MAJCOM for interpretations of the guidance contained in this publication. The authorities to waive wing/unit level requirements in this publication are identified with a tier ("**T-0, T-1, T-2, T-3**") number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, Table 1.1, for a description of the authorities associated with the tier numbers. Submit requests for waivers through the chain of command to the appropriate tier waiver approval authority, or alternatively, to the publication office of primary responsibility (OPR) for non-tiered compliance items. Units have 60 days from above date to comply with this instruction.

SUMMARY OF CHANGES

This document has been substantially revised and needs to be completely reviewed. Major changes include: new requirements for WS3 COMSEC training and documentation, updates to the PDS and COMSEC incident tables, and inclusion of criteria outlined in the new DoDM5210.42_AFMAN13-5011 for PRP/Arming Use of Force standards.

1. General and Systems Information - Responsibilities.

1.1. **Director, National Security Agency (DIRNSA).** The overall management of WS3 material, modules, and associated COMSEC aids is the responsibility of DIRNSA/I551.

1.2. **Air Force Nuclear Weapons Center, Nuclear Systems Division, WS3 Branch, Operating Location San Antonio (AFNWC/NCSW/OL-SA).** AFNWC/NCSW/OL-SA has overall responsibility for procuring, manufacturing, and distributing two-person concept Erasable Programmable Read-Only Memory (EPROM) and Message Processor Hard Drives (MPHD) with associated software.

1.3. **Major Command** (**MAJCOM).** HQ USAFE/A10N is responsible for developing and implementing command WS3 COMSEC policy and doctrine.

1.3.1. HQ USAFE/A10N is the controlling authority (CONAUTH) for WS3 material and maintains responsibility to include:

1.3.1.1. Evaluate COMSEC incidents according to AFMAN 33-283, *Communications Security (COMSEC) Operation and this instruction* and this instruction.

1.3.1.2. Evaluate the security impact involving WS3 COMSEC material when physical incidents affect superseded, current, and reserve material held by the COMSEC account and users.

1.3.1.3. Direct emergency supersession of WS3 COMSEC material held by the COMSEC account and users.

1.4. **COMSEC Account Managers.** The unit COMSEC Account Manager and alternate COMSEC Account Managers act on behalf the Commander and will manage all assigned WS3 COMSEC material assigned for use at their base or installation IAW AFMAN 33-283 and this instruction.

1.4.1. The COMSEC Account Manager must implement a comprehensive user-training program for all WS3 COMSEC Responsible Officers (CRO) and alternates.WS3 COMSEC training will be tailored for WS3 CRO's holding WS3 COMSEC/Controlled Components.

1.4.2. Evaluate all COMSEC incidents/compromises using **Attachment 4** and report IAW paragraph 11**.**

1.5. **WS3 COMSEC Responsible Officer.** Unit Commander will appoint a primary CRO and at least one alternate CRO according to AFMAN 33-283, *Communications Security (COMSEC) Operations*.

1.5.1. The WS3 CROs receive, store, account for, safeguard, control, and destroy WS3 COMSEC material in accordance with this instruction, AFMAN 33-283, and other applicable national, service, and command directives.

1.5.2. Report any known or suspected incidents/compromises involving WS3 COMSEC material/Controlled Components to the COMSEC Account Manager and violating unit's Commander immediately.

1.5.3. The WS3 CRO must implement a comprehensive user-training program for all WS3 COMSEC and controlled components.

1.6. **WS3 COMSEC/Controlled Component Users**.WS3 COMSEC/Controlled Component users have access to material and also the responsibility for safeguarding material. WS3 COMSEC/Controlled Component users will:

1.6.1. Be trained by the WS3 CRO prior to being granted unescorted access to COMSEC materials.

1.6.2. Safeguard WS3 COMSEC material/Controlled Components and control the material until destroyed or turned in.

1.6.3. Be familiar with the types of incidents that could result from improper handling, control, and destruction of WS3 COMSEC material/Controlled Components.

1.6.4. Immediately report any known or suspected incidents/compromises involving WS3 COMSEC material/Controlled Components to the WS3 CRO or COMSEC Account Manager if the WS3 CRO is unavailable.

2. Exceptions. The COMSEC Account Manager will submit written requests for exceptions to the provisions of this instruction to the addresses listed in **Attachment 5**. All requests for exceptions must be accompanied in writing by complete operational justification and an overall mission impact statement. HQ USAFE/A10N will review all requests and waive requirements as necessary.

3. Terms and Definitions.

3.1. **Annual Rekey/Recode.** The annual rekey/recode occurs in the anniversary month of the prior year's rekey/recode and will be accomplished together.

3.2. **Caretaker Status.** A term used for a WS3 installation that has been deactivated pending possible future reuse. A WS3 installation placed into caretaker status may be returned to operational use through the procedures contained in technical order (T.O.) 11N-50-1008, *Deactivation and Reactivation Instructions, Weapons Storage and Security System, AN/FSQ-143 (V).*

3.3. **Coder Transfer Group (CTG).** The CTG is composed of six major components: Code Storage Modules (CSM), Unlock Modules, Recode Modules, Rekey Modules, Universal Release Code (URC) cards and the Code Transfer Unit (CTU). Combined they are capable of storing and transferring unlock codes and encryption keys. It also provides a means to enter and update vault identification (ID) numbers and time delays (TD).

3.3.1. **Code Storage Module.** CSMs are used to store maintenance and mass upload unlock codes for transfer to the Unlock Modules via the CTU. As codes are transferred from the CSMs, they are electronically flagged to prevent reuse.

3.3.1.1. **CSM Access Code.** The access code is a three-digit hexadecimal code that must be entered before information stored in the CSMs may be accessed.

3.3.2. **Code Transfer Unit.** A transportable unit used to electronically transfer the maintenance or mass upload unlock codes from the CSMs or manually enter URC into the Unlock modules for operational use.

3.3.3. **Recode Modules.** Recode modules are used to transfer new unlock codes into the Vault Processor (VP).

3.3.4. **Rekey Modules.** Rekey modules are used to transfer new encryption keys into the Authentication Unit (AU) and Data Authenticator (DA).

3.3.5. **Universal Release Code cards.** URCs are cards with protective technologies packaging that precludes unauthorized access. Sealed in the cards is a three digit hexadecimal code.

3.3.6. **Unlock Module.** Modules are used to store transferred maintenance, mass unlock codes from CSMs (via the CTU) for access to Weapon Storage Vaults (WSV). Unlock Modules are also used to electronically store the transferred hard copy codes from URCs when manually entered into the CTU. Unlock Modules have a storage capacity of either six maintenance unlock codes, one mass upload code, or a URC.

3.4. **Unlock Codes.** Unlock codes are electronic values used to gain authorized access to a WSV. Unlock codes are transferred to the VP from Recode Modules during Recode operations. There are three types of codes: Maintenance Unlock Code, Mass Upload Unlock Code and the URC.

3.4.1. **Maintenance Unlock Code.** A Maintenance code is capable of opening a specific WSV on an installation one time with an imposed time delay for normal maintenance or operational requirements. These codes are vault specific and contain vault ID control data matching the VP ID entered during the ID/TD operation IAW T.O. 11N-50-1005, *Code-Transfer Group OX-69/FSQ-143 (V) Weapons Storage and Security System AN/FSQ-143 (V).* Forty maintenance unlock codes (per WSV) are initially available after a recode operation. Maintenance codes are stored within CSMs and are transferred into Unlock modules for use. Once used, maintenance unlock codes are electronically flagged to prevent reuse.

3.4.2. **Mass Upload Unlock Code.** Codes used to unlock multiple WSVs on a WS3 installation for readiness exercises or operational requirements. A Mass code is capable of opening each WSV on an installation one time with an imposed time delay. Twenty mass upload codes are available after a recode operation. Mass codes are stored within CSMs and are transferred into Unlock modules. Once used, mass codes are electronically flagged in the CSM to prevent reuse.

3.4.3. **Universal Release Code.** Codes designed to be used for operational emergencies only. A URC is capable of opening every WSV on an installation multiple times with no imposed time delay. This code requires special handling and authorization prior to use in accordance with this instruction and Allied Command Operations Directive (AD) 80-6 /USEUCOM Instruction (ECI) 6801.01, *Nuclear Surety Management for the WS3*.

3.4.4. Use USAFE Form 703, *Weapons Storage and Security System (WS3) COMSEC Maintenance Code Tracking* for tracking the number of useable maintenance codes left and the USAFE Form 704, *Weapons Storage and Security System (WS3) COMSEC Mass Code Tracking* for the number of useable mass codes left. Form documentation procedures are provided in the respective attachments to this instruction.

3.5. **COMSEC Terminology.**

3.5.1. **Edition.** A full complement of COMSEC materials. The unique edition number ensures that information in the Recode modules matches that loaded within the CSM and URC.

3.5.1.1. **Effective Edition.** A complete edition (“A” and “B” pairs) of primary and backup sets of Rekey, Recode, CSM, and URC cards. The effective edition is the material currently installed and in use by the WS3.

3.5.1.2. **Reserve Edition.** A complete edition (“A” and “B” pairs) of primary and backup sets of Rekey, Recode, CSM, and URC cards. The reserve editions are on-hand spare editions used to supersede the current effective edition during the scheduled rekey/recode operation or when directed by the CONAUTH.

3.5.1.3. **COMSEC Set.** Each WS3 edition consists of two sets; the Primary and Backup. Each of these sets contains both “A” and “B” Rekey, Recode, CSM, and URC cards.

3.6. **Controlled Components.** Major assemblies, or components within these assemblies, require protection to prevent access by a lone or unauthorized individual. These components are afforded protection under the Two-Person Concept in accordance with this instruction and the specific item technical orders, T.O. 11N-50-1003-1, *Monitor-Indicator Group OD-203/FSQ-143(V) Weapons Storage and Security System*, and T.O. 11N-50-1004, *Processor, Vault Control Group OL-398/FSQ-143(V) Weapons Storage and Security System AN/FSQ-143(V)*. Some components are provided this protection “from cradle to grave” while others only in certain circumstances. **Attachment 3** provides specific handling/protection guidance. Controlled Components alone are not COMSEC material. **Note:** Any Controlled Component loaded with WS3 COMSEC keys/codes is non-trackable COMSEC material and requires two individuals that meet the PRP/Arming Use of Force standards. Once loaded, if compromised, report incidents/compromises per paragraph 11**.**

3.6.1. **Authentication Unit (AU).** The AU is a controlled component when GOLD EPROMs are installed. The AU is located in the WSV and stores keys for the encryption of vault status information being transmitted to the monitoring facilities. Rekey Modules are used to transfer new keys to the AU.

3.6.2. **Vault Processor (VP).** The VP is a controlled component once a GOLD EPROM is installed. The VP is located in the WSV and stores the codes used to access the WS3. The VP also monitors and controls the mechanical operation of the WSV. Recode Modules are used to transfer new code to the VP.

3.6.3. **AU to VP Cable.** This cable interconnects the AU to the VP allowing the exchange of information and data transmission from the WSV to monitoring facilities.

3.6.4. **Data Authenticator (DA).** A controlled component when GOLD EPROMs are installed. DAs are located at both the Local Monitoring Facility (LMF) and Remote Monitoring Facility (RMF). They store keys to decrypt status information transmitted via the AU. Rekey Modules are used to transfer new keys to the DA.

3.6.5. **Motor Starter.** The motor starter (reversing contactor starter) is located within Junction Box 2 of the WSV and controls application of alternating current voltage to the primary drive motor causing upward or downward movement of the WSV.

3.6.6. **Motor Starter Relays (K1, K2, K3).** The motor starter relays are located within Junction Box 1 of the WSV. Application of either the UP or DOWN push buttons causes these relays to close contacts on the motor starter causing upward or downward movement of the WSV.

3.6.7. **Message Processor (MP).** The MP is the computer that interprets all signals received from the WSV and other monitored system components. It translates signals and displays the appropriate message on the operator console along with activating audible alarms.

3.6.7.1. **Message Processor Hard Drive (MPHD).** The MPHD is the controlled component which contains the WS3 computer operating system, WS3 specific alarm program and base maps. The MPHD is installed within the MP for operational use. This component is afforded special handling from “cradle to grave”.

3.6.8. **Alternate Operating System Time Delay Relay.** The time delay relay is located within Junction Box 3 of the WSV and imposes a specified time delay on the Alternate Operating System before operation is allowed.

3.6.9. **Erasable Programmable Read-Only Memory (EPROM).** EPROMs are a field replaceable component of various electronic equipment sub-systems of the WS3. They are used to both store information and physically control basic equipment functions. They exist in two states of control GOLD or BRONZE.

3.6.9.1. **GOLD EPROM.** Any EPROM produced and distributed by AFNWC/NCSW/OL-SA for operational use in WS3 components. To ensure system integrity, GOLD EPROMs require constant Two-Person Concept protection from access by a lone or unauthorized individual.

3.6.9.2. **BRONZE EPROM.** BRONZE EPROMs are installed in components for testing, shipping and storage purposes only.

3.6.9.2.1. These must be replaced with GOLD EPROMs prior to installing the component into an operational system. **Never** install any component equipped with BRONZE EPROMs into an operational system. Operational keys or codes will **never** be loaded into a BRONZE EPROM.

3.6.9.2.2. Unassociated Components in the Forward Supply Point (FSP) (e.g., AU, VP, DA, MP) may have non-controlled BRONZE EPROMs installed. Perform required two person inspections prior to installing GOLD EPROMs in accordance with T.O. 11N-50-1003-1 and T.O. 11N-50-1004.

3.6.10. **Selected Code Transfer Group Components.** The CSM, Rekey, and Recode modules along with the URC cards are controlled components as identified in T.O. 11N-50-1005, *Code-Transfer Group OX-69/FSQ-143 (V) Weapons Storage and Security System AN/FSQ-143 (V).* Collectively these items contain all Unlock codes and encryption key values used by the WS3.

3.7. **Locked Vault.** A WSV is considered locked if upon visual inspection, the WSV is down, the floor box is installed and the "locked" indicator is illuminated on the Shelter Control Panel (SCP) and/or both MPs indicate a code "0" for both "Vault N Open" and "Vault N Unlocked" at the monitoring facilities.

3.7.1. WSV shall not be considered an "Unlocked Vault" during tamper testing conducted IAW 11N-50-1004, if all conditions in 3.7 are met with the exception of floorbox plate removal.

3.8. **Unlocked Vault.** A WSV which does not meet the criteria provided in paragraph **3.7** for a locked vault. When a WSV is placed in access it must be treated as Two-Person Concept until it is locked. An authorized controlled component team must safeguard controlled components at all times when the WSV is not down and locked as specified in paragraph 3.7. This applies even when the vault is physically closed and/or timing out.

3.9. **Time Delay (TD).** The time delay is a classified minimum wait period, mandated by AD 80-6/ECI 6801.01, which is set in both the primary and alternate drive system that must be observed before the vault is raised.

3.10. **Two-Person Concept.** A requirement specified in DOD 5210.41M, *Nuclear Weapon Security Manual/*AFMAN 31-108, *The Air Force Security Manual* and AFI 91-104, *Nuclear Surety Tamper Control and Detection Programs*, to control access to nuclear weapons and related materials.

3.10.1. **Controlled Component Team:** The controlled component team is implemented to protect WS3 COMSEC materials and/or controlled components against access by a lone or unauthorized individual. A lone person will never be left with an unlocked WSV. Doing so will result in a WS3 COMSEC incident. An authorized Controlled Component team consists of at least one COMSEC User as defined below and a second individual who meets one of the following criterions:

3.10.1.1. **COMSEC Users.** COMSEC user is an individual having direct access to WS3 COMSEC, performing maintenance on a WSV, handling WS3 keyed/coded material (e.g., modules), or handling controlled components (e.g., EPROMs, MPHD, and DA). The following applies:

3.10.1.1.1. Certified under the personnel reliability program (PRP) or Arming Use of Force standards as specified in DoDM5210.42_AFMAN13-5011, *Nuclear Weapons Personnel Reliability Program (PRP).* Two interim-certified individuals may not form a WS3 Two-Person Concept/Controlled Component team.

3.10.1.1.2. Capable of detecting incorrect or unauthorized procedures with respect to the tasks being performed.

3.10.1.1.3. Designated via the Access Approval Authority List (AAAL) or Entry Authority List (EAL) to access WS3 COMSEC material or controlled components. See paragraph **4.2**

3.10.1.1.4. Meet training requirements according to section 12.

3.10.1.2. **U. S. Personnel.** Other U.S. personnel, non-WS3 COMSEC trained, fully certified on PRP can perform duties as **one member of the two individuals forming a WS3 Controlled Component team**, but will not be part of a Controlled Component team performing maintenance on the WSV, handling WS3 keyed/ coded material (e.g., modules), or handling controlled components.

3.10.1.2.1. US personnel need not be trained to identify all controlled components or component locations within the WSV. However, they must know that maintenance, adjustment or tampering with the WSV, outside the scope of operations being performed, is not allowed and any unauthorized actions will be reported immediately and treated as a COMSEC incident. During Weapons Loading operations, WSV trained/qualified U.S. personnel may operate the up/down functions of the WSV in the presence of a COMSEC User.

3.10.1.2.2. The WS3 CRO will validate training prior to individuals performing WS3 /Controlled Component team duties. Method for training and training documentation will be devised locally.

3.10.1.3. **Host Nation Personnel**. HN personnel that are fully certified on a NATO equivalent PRP can perform duties as one member of the two individuals forming a WS3 Two-Person Concept team but will not be part of a Two-Person Concept/Controlled Component team performing maintenance on the vault, handling WS3 keyed/coded material (e.g., modules), or handling controlled components.

3.10.1.3.1. HN personnel need not be trained to identify all controlled components. However, because they are not aware of the specific handling/maintenance requirements of each component and its location within the WSV, they must know that no maintenance, adjustment or tampering with the WS3, outside the scope of the operations being performed, is allowed. Any unauthorized actions will be reported immediately and treated as a COMSEC incident. During Weapons Loading operations, WSV trained/qualified HN personnel may operate the up/down functions of the WSV in the presence of a

COMSEC User.

3.10.1.3.2. The WS3 CRO will validate training prior to individual performing WS3 Two-Person Concept team duties. Method for training and training documentation will be devised locally.

3.10.1.4. U.S. personnel performing entry controller duties for an unoccupied exclusion area (with unlocked vault) must know that personnel (U.S. or HN) will not enter an exclusion area without being validated as an authorized WS3 Two-Person Concept team or Controlled Component Team. Any entry by an unauthorized team will result in a COMSEC incident (e.g., emergency response).

3.10.1.5. During exercise situations an authorized WS3 Two-Person Team/Controlled Component Team shall remain with the WSV at any time the PAS is occupied to maintain the integrity of the COMSEC material and controlled components.

3.10.2. **Two signatures required.** WS3 material entered in USTRANSCOM Defense Courier Division (TCJ3-C) will be referred to as "Two Signatures Required" material while it is in the (TCJ3-C) system. This designation will identify the material as necessitating "special handling" during movement to prevent confusion from other articles in the (TCJ3-C) system. These materials must be signed by two authorized personnel when receiving and turning over material to or from (TCJ3-C).

3.10.2.1. **Two-Person Concept Statement:** All (TCJ3-C) forms and inner wrappers of sealed packages must contain the following statement: **"Two-Person Concept as outlined in DOD C-5 210.41-M/AFMAN 31-108 is mandatory at all times for this material. Any unauthorized access by a lone individual is basis for compromise and must be immediately reported to HQ USAFE/A10N and info to DIRNSA/ I551/I413, and HQ AFNIC/ECAP."**

4. Access and Escort Requirements.

4.1. **Access.** Units will establish access controls to ensure only properly authorized personnel with a legitimate need are permitted access to WS3 COMSEC material or controlled components.

4.1.1. Individuals requiring access to WS3 keyed/coded material or controlled components must be US citizens, possess at least a Secret final security clearance, certified through the PRP, and enrolled in the Cryptographic Access Program (CAP) IAW AFMAN 33-283, **chapter 6**, *Cryptographic Access Program* (FOUO).

4.1.2. Physical control (possession) of keyed/coded material, equipment, or controlled components constitutes access.

4.1.2.1. A properly authorized A or B lock individual handling a module/URC from complimentary part of the material while under the direct supervision of authorized individual form the corresponding set (e.g., an individual assigned as a B lock may handle an A lock module while under the direct supervision of an A lock) does not constitute access.

4.1.2.1.1. Direct supervision in this instance means that momentary breaches (e.g., looking away from the individual handling the material to verify the inventory sheet) are authorized given the individual does not have the opportunity to tamper with the item.

4.1.3. Viewing of WS3 COMSEC material and/or controlled components does not constitute access.

4.1.4. Personnel under escort by an authorized team are not considered to have access.

4.2. **Access Authority Approval Listing (AAAL)/Entry Authority List (EAL).**

4.2.1. The AAAL or EAL will designate personnel authorized to access, issue, and receive Effective edition modules and URCs in accordance with this instruction and AFI 21-200, *Munitions and Missile Maintenance Management,* DOD 5210.41M/Air Force Supplement, *Nuclear Weapon Security Manual* and AD 80-6 /ECI 6801.01.

4.2.2. The AAAL or EAL may be used to designate personnel authorized to access, issue, and receive controlled components and non-trackable COMSEC (e.g., DAs) in accordance with this instruction and AFI 21-200, *Munitions and Missile Maintenance Management,* DOD 5210.41M/Air Force Supplement, *Nuclear Weapon Security Manual* and AD 80-6 /ECI 6801.01.

4.2.3. The owning WS3 CRO will sign any AAAL/EAL used to grant access to WS3 COMSEC material and/or controlled components.

4.2.4. The AAAL/EAL fulfills the requirement from AFMAN 33-283, chapter 7 for an Effective edition WS3 COMSEC access list.

4.2.5. Designate personnel on the AAAL (used to access Effective edition modules and URCs) as either the “A” or “B” lock.

4.2.5.1. Personnel are restricted from any position/designation/authorization that could provide access to the complimentary part of the material. Once assigned as an “A” or “B” lock they cannot change to the complimentary lock until the edition that they had access to is superseded.

4.2.5.2. If reassigned to another base where duties require WS3 COMSEC access, personnel may be assigned as either “A” or “B” lock regardless of their designation at a previous unit.

4.2.6. Limit to the extent possible, consistent with mission requirements, the number of personnel having access to WS3 COMSEC material and/or controlled components.

4.2.7. WS3 CROs must review any AAAL/EAL used to grant access to WS3 COMSEC material and/or controlled components monthly to ensure accuracy and then annotate the review date, month, and their initials on the list. Only one copy of each AAAL/EAL must be reviewed.

4.3. **Escort Requirements:** Personnel not authorized access to Effective edition WS3 COMSEC material and/or controlled components will be escorted into areas where these components are exposed. These personnel will remain under the constant supervision of an authorized Two-Person Concept team or Controlled Component Team and are restricted from having access to WS3 COMSEC material and/or controlled components (physically handling or controlling any materials).

4.3.1. The AAAL/EAL will designate those individuals authorized to escort (escort officials) visitors viewing Effective edition WS3 COMSEC material and/or controlled components.

4.3.2. Before allowing viewing of WS3 COMSEC material and/or controlled components, the escort official will positively identify visitors by comparing personal identification cards with either approved COMSEC viewing letter, team composition/site visit messages, properly authenticated EALs, or other official notification of visit as defined in paragraph 4.3.4.

4.3.3. Use AF Form 1109, *Visitor Register Log*, to record the arrival and departure of visitors granted escorted entry to areas containing exposed WS3 COMSEC material and/or controlled components. Retain the AF 1109 on file for 1 year after date the last visitor was recorded on the form.

4.3.3.1. Personnel not designated on AAAL/EAL used to grant access to WS3 COMSEC material and/or controlled components and whose duties normally require them to be present in the area where a security container containing WS3 material is located (e.g., Monitoring Facility Operator, Munitions Controller, Emergency Action Controllers, MASO), do not need to be recorded on an AF Form 1109. These personnel are restricted from having access to WS3 COMSEC or controlled components (physically handling or controlling any materials).

4.3.4. Official inspection teams from MAJCOM, Headquarters Air Force (HAF), Defense Threat Reduction Agency (DTRA), etc. are authorized escorted entry into areas containing WS3 keyed/coded material and controlled components in the performance of their official duties. Inspectors do not require PRP certification, but must be U.S. citizens and possess a final security clearance commensurate with the material being viewed.

4.4. **Reserve/Superseded Editions.** Access and escort requirements to Reserve and Superseded editions of WS3 COMSEC material stored in the COMSEC holding account will be stored in accordance with Two-Person Integrity procedures. COMSEC accounts will use the EKMS or KMI computer generated TPC/TPI inventory forms or the AF Form 4167 to account for all reserve/superseded editions.

5. Classification and Management of COMSEC Material. General COMSEC classification guidance may be found in AFMAN 33-283. Additionally, the following guidance applies to the COMSEC components of the WS3:

5.1. Refer to **Attachment 3** for specific guidance on classification and handling of WS3 COMSEC material and/or controlled components. This table cannot address all circumstances that might arise while handling material. In those cases, always handle the material/circumstance by the most restrictive means available, and the COMSEC Account Manager will seek guidance/clarification from the CONAUTH.

5.2. **Unlock Modules.** Storing loaded Unlock Modules bypasses additional security features associated with the Code Storage Module (CSM access code). Unit Commander must be aware of the additional risk and grant authorization (e.g. written/verbal notification, unit plans) to return loaded Unlock Modules to storage. If loaded Unlock Modules are returned to storage, they must be added to the USAFE Form 701**,** *Weapon Storage and Security System (WS3) COMSEC Inventory*.

5.2.1. Unlock Modules must be erased when the codes they contain are no longer required. This will be documented on the USAFE Form 702 *Weapon Storage and Security System (WS3) COMSEC Module Issuing Log*.

5.3. **Universal Release Codes.** URC cards will only be issued or used when properly authorized in response to actual contingency operations in accordance with AD 80-6/ECI 6801.01. Specify these procedures and authority for use in unit plans, OIs and checklists.

5.3.1. Do not issue or use URCs for readiness exercises or system rekey/recode operations.

5.3.2. In the event a URC is compromised or opened during a higher state of alert or readiness, and a subsequent peacetime posture is declared, request authorization IAW paragraph 17.3 or 17.3.1 to initiate a system rekey/recode using the Reserve edition as soon as possible.

6. Physical Security of WS3 COMSEC and Controlled Components.

6.1. Use requirements in **Attachment 3** to protect and control all WS3 COMSEC material and/or controlled components in a manner to prevent a lone or unauthorized individual from having access. This is accomplished by properly storing and accounting for the material and components and application of Two-Person Concept procedures.

6.2. **Security Container Requirements**: Store WS3 COMSEC material and/or controlled components in a General Services Administration (GSA) approved security container with either an electromechanical combination lock that is capable of holding two independent combinations (e.g., MAS-Hamilton X-08/X-09) or two three-position dial combination locks installed.

6.2.1. Consider individual drawers of a multiple-drawer safe as separate security containers only if each drawer is a locking drawer equipped with required, serviceable locks.

6.2.2. All safe drawers must be installed and locked to consider the safe as secured. Immediately remove from service any safe with questionable serviceability. Never lock WS3 COMSEC material and/or controlled components in a security container drawer if the serviceability of the lock is questionable.

6.3. **Security Container Combinations**: Each security container used to store WS3 COMSEC material and/or controlled components will have an “A” combination and a “B” combination installed and known only by authorized individuals. At no time will one person know, or have access to, both combinations. Do not use the same combinations for two separate security containers in the same facility. This restriction also applies to separate locking drawers in a safe.

6.3.1. **Combination Changes.** Authorized individuals must change security container combinations when:

6.3.1.1. The lock is initially placed into use.

6.3.1.2. At least once a year.

6.3.1.3. The combination has been compromised.

6.3.1.4. A person knowing the combination is no longer authorized access (e.g., removed from the AAAL/EAL) for any reason other than death.

6.3.1.4.1. It is not necessary to change combinations if an individual is suspended from PRP, providing they remain on the AAAL/EAL. Unit Commander will direct a combination change if the determination is made that WS3 COMSEC material and/or controlled components are in jeopardy.

6.3.1.5. When any repair work has been performed on the safe combination lock.

6.3.1.6. When a container certified as locked is found open to include any containers with standard forms (SF) 700, *Security Container Information*, stored in the unlocked safe.

6.3.2. **Combination Documentation.** Each safe combination will have a separate SF 700 and SF 702, *Security Container Check Sheet*. Do not store a completed SF 700 in the container for which it applies.

6.3.2.1. Complete each SF 700 per the instructions on the form clearly marking the outside with which Edition/Set combination it contains, and the correct classification.

6.3.2.2. The SF 700 with the combinations for the Effective Primary container will be stored in the Effective Backup container and vice versa.

6.4. **Effective Edition Storage:** Store IAW AD 80-6/ ECI 6801.01 and as follows:

6.4.1. **Modules:** The Primary and Backup module sets must be stored within GSA-approved safes located at separate facilities (e.g. different buildings).

6.4.2. **URCs:** Store the Effective edition URCs within GSA-approved safes at facilities equipped with a duress alarm and manned 24-hours a day

6.4.2.1. URC cards from the Primary and Backup sets may be stored in the same facility.

6.4.2.2. At no time will both the Effective edition "A" and "B" URC cards be stored within the same facility.

6.4.2.3. URCs may be stored in the same container as the Primary/Backup module sets.

6.5. **Reserve Edition Storage:** Store as follows:

6.5.1. Multiple Reserve editions may be stored in the same container.

6.5.2. Reserve editions of keyed/coded material will be stored within the COMSEC account separate from the Effective edition.

6.6. **Rekey/Recode Operation:** Units may begin treating the Reserve edition as Effective material, with respects to storage, at any point during the week prior to beginning the rekey/recode operation. Once installed in the DA, the material formally becomes a second Effective edition and will be stored in accordance with paragraph **6.4**

6.6.1. Both the current and new Effective editions may be stored together within the same containers until the rekey/recode operation is completed.

6.6.2. The WS3 CRO will verify successful completion of the rekey/recode operation prior to supersession of the outgoing Effective edition. This may be accomplished by reviewing events files at the completion of all operations or being present for the rekey/recode operation at each vault.

6.7. **Superseded Material:** Superseded modules will be stored in the same manner as Reserve material until returned to DIRNSA. Destroy superseded URCs IAW paragraph **9**. As soon as mission requirements permit, return superseded material to the COMSEC Account Manager for storage.

6.8. **Controlled Components.** Store Controlled components within a GSA-approved safe. Controlled components may be stored in the same safe drawer as WS3 COMSEC materials. See paragraph **21** and **Attachment 3** for additional storage and handling instructions.

6.8.1. Store unassociated components (e.g., AU, VP, DA, MP) IAW T.O. 11N-50-1003-1 and T.O. 11N-50-1004. These items do not require Two-Person concept before two person inspection or after GOLD EPROMs are removed IAW T.O. 11N-50-1003-1 and T.O. 11N-50-1004.

6.8.2. VPs are classified Secret Not Releasable to Foreign Nationals (NOFORN) after they have been installed in an operational vault, electrical power has been applied and recode operation has been performed. The VP remains classified until GOLD EPROMs U18 and U11 have been destroyed or code set is superseded and must be stored in the same manner as Effective Edition. (Note: When U18 is destroyed, the VP must be returned for rework.)

6.8.2.1. If the VP is removed from a WSV, it may be temporarily stored IAW paragraph 6.2 to allow reuse.

6.8.3. AUs are classified Secret-Crypto/NOFORN after they have been installed in an operational vault, electrical power has been applied and rekey operation has been performed. It becomes unclassified in the event of power loss. However, they still require Two Person Control to prevent tampering until GOLD EPROMs are removed.

6.8.3.1. If the AU is removed from a WSV, it may be temporarily stored IAW paragraph 6.2 to alleviate removal/destruction of GOLD EPROMs.

6.9. **Handling.** An individual “A” or “B” module/URC does not require handling under the Two-Person Concept. See **Attachment 3** for specific WS3 COMSEC material and/or controlled component handling requirements.

6.9.1. When a security container containing WS3 COMSEC materials is accessed, personnel designated as “A” lock are responsible for safeguarding the “A” material within and likewise the “B” lock must safeguard any “B” material until the security container is secured.

6.10. **Unlock Modules.** Empty unlock modules are not COMSEC material and are Unclassified. Once loaded, unlock modules become SECRET/NOFORN until erased.

6.10.1. Track loaded Unlock Modules on a USAFE Form 702.

6.10.2. Loaded unlock modules may only be issued to a corresponding A or B designated individual.

6.11. **CSM Access Code Management.** CSMs arrive from DIRNSA with an UNCLASSIFIED shipping access code of "FFF" installed. Once changed from the shipping code, the CSM access code is classified SECRET/NOFORN.

6.11.1. The CSM access code must be changed when:

6.11.1.1. The material becomes the Effective Edition.

6.11.1.2. When a person knowing the CSM access code is no longer authorized access (e.g., removed from the AAAL/EAL).

6.11.1.2.1. It is not necessary to change the code if an individual is suspended from PRP, providing they remain on the AAAL/EAL. The Unit Commander may direct a code change if the determination is made that WS3 material is in jeopardy.

6.11.1.3. When the CSM access code is compromised.

6.11.2. Complete a separate SF 700 for each CSM access code using procedures in **Attachment 6**.

6.11.3. The SF 700 for the Effective Primary CSMs must be stored with the Effective Backup modules and vice versa.

6.12. **Safe Lockout Procedures.** In the event a safe used to store WS3 COMSEC material and/or controlled components cannot be opened; take the following actions:

6.12.1. Notify the WS3 CRO and COMSEC Account Manager.

6.12.2. Follow local procedures to contact a locksmith.

6.12.3. For WS3 COMSEC material; a designated "A" and "B" team will remain in the area of the safe at all times while forcible entry is being attempted.

6.12.4. For controlled components; an authorized Two-Person Concept team will remain in the area of the safe at all times while forcible entry is being attempted.

6.12.5. Due to possible damage to the material stored within, torching will be used only as a last resort.

6.12.6. After the team accesses the safe, assess the damage and immediately safeguard/store the material in accordance with paragraph **6.** COMSEC Account Manager will report any damaged material using the appropriate addresses listed in **Attachment 5**.

7. Inventory Procedures for WS3 COMSEC Material.

7.1. **Effective Edition:** Use USAFE Form 701, *Weapon Storage and Security System (WS3) COMSEC inventory*, for inventory of all effective WS3 COMSEC materials. Inventories listing WS3 COMSEC materials are FOUO. Inventory WS3 COMSEC material as Accounting Legend Code (ALC)-1 material in accordance with AFMAN 33-283, and this instruction.

7.1.1. Perform an inventory each day the container is opened just prior to final closing. For consecutive shifts within the same day, inventory all material at the end of each shift in which the safe was opened. As a minimum, conduct inventories of Effective edition material at least once each month, prior to change of WS3 CRO or COMSEC Account Manager, or when directed by CONAUTH.

7.1.2. A designated "A" and "B" Two-Person Concept team will conduct the inventory. Both individuals will verify all information off the material against the appropriate USAFE Form 701 entry.

7.1.3. Procedures for completing USAFE Form 701s are contained in **Attachment 8**.

7.1.4. The WS3 CRO must review all USAFE Form 701s monthly to ensure they are accomplished correctly. Document these reviews in accordance with **Attachment 8**.

7.1.5. Maintain USAFE Form 701s for 6 months plus the current inventory.

7.1.6. Erased unlock modules are not COMSEC material and will not be inventoried on a USAFE Form 701.

7.1.7. COMSEC Account Manager Semi-Annual Inventory. The COMSEC Account Manager and will conduct and document a semi-annual inventory of all WS3 COMSEC material in accordance with AFMAN 33-283. This will include a complete and detailed review of all related accountability and training documentation and a physical inventory of all Effective edition material. A designated "A" and "B" Two-Person Concept team from the WS3 COMSEC User will accompany and facilitate this inventory.

7.2. **Reserve and Superseded Editions.** Inventories of Reserve edition and Superseded material stored within the COMSEC account are the responsibility of the COMSEC Account Manager. Inventories will be conducted semi-annually or on days the safe is opened, prior to change of COMSEC Account Manager, or when directed by CONAUTH.

8. Issue Procedures for WS3 COMSEC modules and URC cards.

8.1. Use the USAFE Form 702, *Weapon Storage and Security System (WS3) COMSEC Module Issuing Log*, to record the issue, transfer, erasure, subsequent turn-in, and destruction of WS3 COMSEC Effective Edition Material. Completed USAFE Form 702s are FOUO. Maintain them for 6 months plus the current record.

8.2. Use procedures in **Attachment 7** to document the issue, transfer, erasure, subsequent turn-in, and destruction of WS3 COMSEC Effective Edition Material. WS3 material transferred from the CSM to unlock modules and subsequently stored in the WS3 COMSEC safe will be annotated on the USAFE Form 702 as "Turned In" but not "Erased".

8.3. Local transfer of modules or URCs between assigned personnel is authorized provided the transfer is coordinated with, and approved by, an individual authorized on the unit AAAL to issue modules/URCs prior to the actual transfer.

8.4. URCs may only be issued for use when authorized IAW AD 80-6/ ECI 6801.01.

9. Destruction of WS3 COMSEC.

9.1. The only WS3 COMSEC materials authorized for local destruction are superseded URCs. Destruction of URCs is only authorized by DIRNSA approved destruction devices. Consult the COMSEC Account Manager for listing of DIRNSA approved destruction devices.

9.2. Accomplish destruction within 72 hours of supersession. Document the destruction on the SF 153, *COMSEC Material Report*. This form is FOUO. Maintain SF 153 for 3 years after destruction.

10. Inspection and Reporting Damage or Tampering of WS3 COMSEC.

10.1. **Inspection Requirements.** Upon initial receipt, inspect modules and URCs for serviceability, signs of possible tampering and sabotage in accordance with T.O. 11N-50-1005.

10.2. Removed damaged modules from service and report to appropriate addresses listed in **Attachment 5**.

10.3. If evidence of tampering or sabotage is detected remove COMSEC material from service and report in accordance with paragraph **11**. Maintain/store the material under Two-Person Concept as applicable until further instructions are received from the CONAUTH.

11. Reporting WS3 COMSEC Incidents

11.1. **COMSEC Incident.** In accordance with AFMAN 33-283, a COMSEC incident is an occurrence involving a failure to follow established COMSEC instructions, procedures, or standards. Incidents are categorized as follows:

11.1.1. **Practice Dangerous to Security (PDS).** A procedure that has the potential to jeopardize the security of COMSEC material if allowed to continue.

11.1.1.1. A WS3 COMSEC PDS will **normally not** result in the CONAUTH directing the involved unit to perform a system-wide rekey/recode.

11.1.2. **COMSEC Incident.** An occurrence that jeopardizes the security of COMSEC material or the secure electrical transmission of national security information. Incidents are evaluated by the CONAUTH as either "No Compromise" or "Compromise”.

11.1.2.1. A WS3 COMSEC incident **may** result in the CONAUTH directing the involved unit to perform an immediate system-wide rekey/recode.

11.2. **Incident Responsibilities.** Personnel at all levels who access WS3 COMSEC must immediately report to the WS3 CRO or the COMSEC Account Manager (when the WS3 CRO is not available) any circumstances, intentional or inadvertent, which could lead to the unauthorized disclosure of classified information, including its loss, improper use, unauthorized viewing, or any other instance that could possibly jeopardize the value of COMSEC material.

11.2.1. Any person or activity **detecting** or **suspecting** a COMSEC incident is responsible for immediately reporting in accordance with this instruction and AFMAN 33-283. Any evidence of a failure to immediately report an incident will be immediately and thoroughly investigated by the COMSEC Account Manager and included in any subsequent incident reporting.

11.3. **Incident Evaluation**. Upon discovery of an incident, the WS3 CRO and COMSEC Account Manager will use both the overarching guidance and procedures provided in AFMAN 33-283, and the specific PDS and Incident tables in **Attachment 4** of this instruction to determine what, if any, type of report is required.

11.3.1. The PDS and Incident Tables in **Attachment 4** were developed specifically for WS3 COMSEC and are much more detailed than the corresponding tables in AFMAN 33-283. While they are not intended to be all encompassing, they include the most common incidents encountered and provide a very solid base for WS3 CROs and COMSEC Account Managers to determine reporting. Where there is a perceived conflict between this instruction and the AFMAN, immediately contact the CONAUTH for resolution prior to reporting.

11.3.2. Use the guidance in AFMAN 33-283 for sample report formats.

11.4. **PDS Reporting.** PDS as described in table A4.1., Rule 1 will require that a physical report be forwarded to the CONAUTH within 3 duty days of discovery using addresses in **Attachment 5**. The CONAUTH may render an evaluation on a PDS. PDS as described in table A4.1., Rule 2 do not require coordination outside the unit.

11.4.1. The violating unit, through their COMSEC Account Manager, is required to respond to all questions put forth by the CONAUTH. An inquiry is not required for a PDS unless requested by the CONAUTH, violating unit's commander, or COMSEC Account Manager.

11.4.2. The CONAUTH will notify the COMSEC Account Manager if further action or information is required on PDS reports.

11.5. **Incident Reporting.** The COMSEC Account Manager will send an incident report to the applicable addresses listed in **Attachment 5** within 24 hours after incident discovery or receipt of amplifying information.

11.6. **Compromised Modules.** Handle compromised modules as follows:

11.6.1. Users and COMSEC Manager will retain all compromised modules under Two-Person Concept unless explicit instructions are provided by the CONAUTH.

11.6.2. Request disposition instruction from the CONAUTH using addresses listed in **Attachment 5**. After receiving disposition instructions, package according to paragraph **18.**

12. WS3 COMSEC Training.

12.1. Training at all levels shall stress that the ultimate success or failure of COMSEC programs rests with the material's end user. The careless user or the user who fails to follow procedures for using, safeguarding, and destroying COMSEC material wastes all security efforts. COMSEC users must ensure that anyone who receives COMSEC material is authorized and their security clearance is verified. Users must follow all security rules at all times and immediately report any incidents to their WS3 CRO and/or COMSEC Account Manager.

12.1.1. Personnel who do not complete all required training/reading by the end of the month due will be removed from the AAAL/EAL and will not be placed back on an AAAL/EAL until all required training/reading is complete. Personnel on leave or temporary duty (TDY) are not required to be removed from the AAAL/EAL provided they complete this training/reading within 5 duty days of return to duty section and prior to accessing WS3 COMSEC material.

12.2. **COMSEC Account Manager Responsibilities.** The COMSEC Account Manager will train all WS3 CROs and alternates both initially and provide annual refresher training on overarching COMSEC responsibilities and requirements in AFMAN 33-283.

12.3. **WS3 CRO Responsibilities.** The WS3 CRO will develop a comprehensive training program. Training requirements are as follows:

12.3.1. WS3 CROs will provide initial and annual refresher training to all other WS3 CROs on USAFEI 33-283 **Attachment 2** items.

12.3.1.1. WS3 CROs will provide training to all WS3 COMSEC and controlled component users. As a minimum this must include: overarching COMSEC responsibilities and requirements in AFMAN 33-283, items listed in **Attachment 2** of this publication, associated manuals and reference material, and applicable unit procedures (e.g., plans, OIs, and checklists).

12.3.2.1. The WS3 CRO will conduct initial and annual training for each individual prior to being authorized access to WS3 COMSEC material or controlled components.

12.3.2.2. Non-COMSEC users identified in paragraphs 3.10.1.2. and 3.10.1.3. may receive tailored training to adequately perform duties.

12.3.2.3. Verify all training/reading is current prior to addition to AAAL/EAL and in conjunction with AAAL/EAL monthly reviews.

12.3.2.4. Ensure individuals are enrolled in the Cryptographic Access Program (CAP) as outlined in AFMAN 33-283.

12.4. **User Responsibilities**. Users with authorized access to WS3 COMSEC material and controlled components must know how to handle, control, inventory, use, secure and report incidents. Complete all required COMSEC training/reading before accessing WS3 COMSEC material and controlled components.

12.5. **Required Reading.** Personnel authorized access to WS3 COMSEC material and controlled components will review applicable portions of AFMAN 33-283, this publication, associated manuals and reference material, and applicable unit procedures (e.g., plans/OIs/checklists).

12.5.1. Required reading will be performed semi-annually and may be performed in conjunction with initial and annual WS3 COMSEC training.

12.6. **Training Documentation.**

12.6.1. Initial and refresher training covering AFMAN 33-283 items will be documented on an AF4168, *COMSEC Responsible Officer and User Training Checklist*.

12.6.2. Initial and refresher training covering USAFEI 33-283 **Attachment 2** items will be documented by having both the trainer and trainee print, sign, and date in the spaces provided at the bottom of Attachment 2.

12.6.2.1. Semi-annual WS3 COMSEC required reading will be tracked on documentation developed by the WS3 CRO which allows user to sign and date completion.

12.6.3. WS3 COMSEC Emergency Action Plan (EAP) reviews and exercises will be tracked on documentation developed by the WS3 CRO.

12.6.4. WS3 CROs and Users are required to maintain current training documentation only.

12.6.5. At a minimum WS3 communications personnel (e.g., authorized access to Controlled Component loaded with WS3 COMSEC keys/codes) will be trained on all "*" items listed in **Attachment 2** and complete semi-annual reading IAW paragraph 12.5. Document all training and reading requirements IAW paragraph 12.6.

13. Emergency Evacuation and Disablement Procedures.

13.1. With proper notification, authority, or if a situation arises requiring emergency evacuation (EE) or emergency disablement (ED) procedures, "lock down" all WS3 equipment and associated classified COMSEC items (with possible exception of the URCs) within a WSV.

13.1.1. Upon completion of the EE and/or ED of all assigned weapons, a Two-Person Concept Team will transport the remaining Effective edition WS3 COMSEC materials to a predetermined WSV for storage and "lock down".

13.1.2. The unit will immediately contact the CONAUTH for disposition instructions for the Effective edition URCs.

13.2. The next available Two-Person Concept team (one of whom must be a WS3 CRO or alternate WS3 CRO) will transport the WS3 COMSEC material (Reserve and Superseded editions) from the COMSEC account to a predetermined WSV for storage and "lock down".

13.2.1. Normally, the COMSEC account will have the SF 153 ready for issuing to the WS3 CRO and WS3 team member when they pick up the WS3 material. Only during an emergency situation where time and circumstances do not permit, will the receiving WS3 CRO and WS3 team member annotate a Memorandum for Record (MFR) and sign the front or back of the USAFE Form 701 to acknowledge receipt of the material. The WS3 CRO and WS3 team member will properly accomplish the SF 153 when time and circumstances permit.

13.3. All COMSEC materials and equipment may be stored within one WSV during these contingencies if room permits.

14. COMSEC Requisitioning.

14.1. DIRNSA/I551/I5171/I513 produces and distributes WS3 material to the appropriate COMSEC account for each WS3 installation. Annual deliveries of material will normally consist of a single edition, which is the new second Reserve edition for each location.

14.2. Each unit will maintain one Effective and at least two Reserve editions of WS3 COMSEC material. When a unit performs their annual rekey/recode, one Reserve edition will be issued to the WS3 CRO and the superseded edition will be returned to the COMSEC Account Manager until disposition instructions are received from the CONAUTH. Until a resupply edition is received the unit will only be required to maintain one Reserve edition.

14.3. The CONAUTH will send a message to the applicable addresses listed in **Attachment 5** requesting material production and distribution. This request is completed by the

CONAUTH following notification that a rekey/recode operation has been completed. This action is not required if the unit has two Reserve editions of WS3 COMSEC material on-hand.

15. Receipt of COMSEC Material, Unit Procedures.

15.1. **COMSEC Account Manager Responsibilities**. Upon receipt of WS3 COMSEC material, the COMSEC Account Manager will process the material under Two-Person Concept. Two individuals will process and issue WS3 COMSEC material in accordance with AFMAN 33-283.

15.1.1. The COMSEC Account Manager will notify the WS3 CRO of receipt of Reserve WS3 COMSEC material so they may inspect code modules for evidence of tampering and accomplish code module receipt procedures within 72 hours of arriving on station.

15.1.2. Following COMSEC account addition and WS3 User receipt inspection procedures completion, the COMSEC Account Manager will send a memorandum to the CONAUTH identifying a new reserve edition is on hand and serviceable.

15.2. **Receipt Inspection**. Receipt inspection will be performed within 72 hours of arrival on station. The COMSEC Account Manager may either temporarily issue the edition to the WS3 CRO or the receipt inspection can be accomplished by the WS3 CRO, in the presence of the COMSEC Account Manager, at the COMSEC account without requiring the temporary issue procedure.

15.2.1. The Reserve edition is identified by loading the unit ID/TD into each of the designated sets. Refer to T.O. 11N-50-1005 for inspection and ID/TD procedures.

15.2.2. Remove URCs from plastic shipping sleeve, inspect URCs for evidence of tampering or damage and then return them to the plastic shipping sleeve for added protection.

15.2.3. It is not required to change the CSM access code during the receipt inspection.

15.2.4. Upon completion of the inspection, the WS3 CRO will return the Reserve edition to the COMSEC Account Manager until needed for operational use (e.g., annual recode/ rekey).

16. WS3 COMSEC Account Manager Issue Procedures.

16.1. The COMSEC Account Manager will utilize procedures outlined in AFMAN 33-283 and this instruction for the issue of WS3 materials to the WS3 User.

16.2. Issue WS3 COMSEC material under Two-Person Concept procedures. At least one of the two individuals signing the SF 153 must be a WS3 CRO or Alternate WS3 CRO.

17. Implementing WS3 COMSEC Material.

17.1. **Backup Set.** The Effective Backup sets of Rekey, Recode, and CSMs are only used when a failure or malfunction of the Effective Primary set occurs, notify the CONAUTH when this occurs.

17.2. **Reserve Edition.** Units are authorized to implement the Reserve edition of WS3 material during the annual Rekey/Recode without further CONAUTH approval.

17.3. Units must receive authorization from the CONAUTH prior to implementing the Reserve edition of WS3 material for any reason other than the anniversary month.

17.3.1. In response to operational emergencies, where prior coordination with the CONAUTH is not possible, the WS3 User commander is authorized to direct implementation of the Reserve edition of WS3 material.

17.3.2. After implementation, the COMSEC Account Manager will notify the applicable addresses listed in **Attachment 5** via SIPR message (short title and/or edition is not required) fully detailing the date, time, and reason for implementation of the Reserve edition.

17.4. Following completion of successful rekey/recode, the WS3 CRO will submit a classified CONFIDENTIAL memorandum to the unit COMSEC Account Manager, identifying that rekey/recode operations have been completed.

17.4.1. This memorandum must include the following:

17.4.1.1. The edition that was superseded and removed from WSV (e.g., “CG”).

17.4.1.2. The new Effective edition that was installed in the WSV (e.g., “FL”).

17.4.1.3. The date the rekey/recode operation began.

17.4.1.4. The date the rekey/recode operation was completed.

17.4.1.5. The identification of new Reserve edition (e.g., “HF”).

17.4.1.6. A statement requesting a new replacement edition.

17.4.1.7. A statement indicating whether or not the superseded edition’s modules were compromised prior to the rekey/recode. If so, include a reference to the COMSEC Incident report that was submitted for them.

17.4.2. The base COMSEC Account Manager will forward this information to the CONAUTH along with a request for disposition of the superseded edition. The CONAUTH will use this memorandum to provide disposition instructions and also requisition a new Reserve edition from DIRNSA.

18. Routine Turn-In of WS3 COMSEC Material.

18.1. For return of superseded WS3 COMSEC materials to DIRNSA/I5171:

18.1.1. The COMSEC Account Manager will notify the CONAUTH by SIPR message that superseded WS3 COMSEC material is available for return. This notification is accomplished by completing the memorandum identifying that rekey/recode operations were completed in accordance with paragraph 17.4. Maintain this memorandum for 1 year.

18.1.2. The CONAUTH will provide the necessary disposition instructions to the COMSEC Account Manager via the applicable addresses listed in **Attachment 5**. This message will include authorization to return the superseded edition.

18.1.3. The COMSEC Account Manager will package the WS3 material for return shipment to DIRNSA/I3171 IAW with DoD 5200.1 V, AFI 31-401, *Information Security*

Program Management, AFMAN 33-283, U.S. Transportation Command Defense Courier Division Customer Service Guide and as follows:

18.1.3.1. **Inner Package.** Place the "A" and "B" WS3 materials into separate inner packages.

18.1.3.1.1. Using tamper evident tape seal each package so that any tampering or attempted tampering will be evident.

18.1.3.1.2. Label all sides of the outside of each package "A" or "B" accordingly.

18.1.3.1.3. Place receiver and sender address (complete physical) labels on each package and stamp with appropriate classification markings.

18.1.3.1.4. Place TPC statement from paragraph **3.10.2.1** and any other special handling instructions on the same side as the address labels.

18.1.3.1.5. Accomplish a separate SF 153 (e.g., one "A" and one "B") identifying the material contained within each package. Annotate "Authority for transfer is HQ USAFE/ A10NM message date-time-group (DTG) #######" on the SF 153.

18.1.3.1.6. Enter the required Two-Person Concept statement on each SF 153 in accordance with paragraph **3.10.2.1**

18.1.3.1.7. Insert each completed SF 153 in an envelope marked "A" or "B" as appropriate.

18.1.3.2. **Outer Package**. Place inner packages and SF 153 envelopes into outer package.

18.1.3.2.1. Seal and wrap outer package according to DCS guidance.

18.1.3.2.2. Mark the package with the Transportation Control Number (TCN), (block 40 on DD Form 1384, *Transportation Control and Movement Document*) and the statement "Two Signatures Required".

18.1.3.2.3. Complete DD Form 1387, *Military Shipment Label*, per DCS customer guide.

18.1.3.2.4. Ensure that "Two Signatures Required" is places in block 14 for entire shipment or block 43b for individual packages.

18.1.3.2.5. Include the statement: **"Material must be receipted for at destination address by any one individual from the A personnel group and any one individual from the B personnel group**."

18.1.3.3. Produce a memo for the DCS couriers requesting they contact an authorized individual at DIRNSA/I5171 for pick-up.

18.1.3.4. Transport the package under Two-Person Concept procedures to the DCS station for delivery. Ensure two team members sign entering the package into DCS channels and two DCS personnel receipt for the package.

18.1.3.5. Compromised WS3 COMSEC material will be handled/packaged the same, but shipped according to CONAUTH guidance.

19. Transfer of WS3 COMSEC Material.

19.1. All transfers of WS3 COMSEC material from one COMSEC account to another, except as specifically authorized in this instruction, require CONATH approval. Under no circumstances will WS3 COMSEC material containing any unit's Effective edition be transferred to another account.

20. Caretaker Status and Training Code Transfer Group Requirements.

20.1. Training/Caretaker CTG material must be protected and tracked as ALC-4 material and is unclassified NOFORN.

20.2. When Training/Caretaker CTG material is no longer required notify the CONAUTH for disposition instructions.

20.3. Do not destroy Training/Caretaker CTG modules.

20.4. Units may develop local procedures to track Training/Caretaker CTG material provided the following are met:

20.4.1. Store Training/Caretaker CTG material in accordance with **Attachment 3**.

20.4.2. Inventory Training/Caretaker CTG on a monthly basis**.** Use serial number of components for accountability purposes. If inventory discrepancies cannot be resolved, notify the CONAUTH.

20.4.3. Training/Caretaker CTG material is tracked as ALC-4 material.

21. Management of WS3 Controlled Components.

21.1. **Protection and Control**. Protect and control all identified WS3 controlled components in such a manner as to prevent access by a lone or unauthorized individual in accordance with **Attachment 3** of this instruction and T.O. 11N-50-1003-1, T.O. 11N-50-1004, T.O. 11N-50-1005, T.O. 11N-50-1006, and T.O. 11N-50-1008.

21.1.1. Institute and enforce the Two-Person Concept IAW paragraph 3.10.1 to prevent access by a lone or unauthorized individual.

21.1.2. Access to controlled components is defined in paragraph 4.1.

21.1.3. Designate personnel authorized to access to controlled components IAW paragraph 4.2.

21.1.4. Escort personnel without authorized access to controlled components IAW paragraph 4.3.

21.2. **Controlled Component Training.** Train all personnel with access to controlled components IAW paragraph 12.

21.3. **Physical Security and Accountability.** Store controlled components according to paragraph 6.

21.3.1. Use USAFE Form 31, *Weapons Storage and Security System (WS3) Controlled Component Inventory*, to inventory all unassociated controlled components.

21.3.1.1. Procedures for completing USAFE Form 31s are contained in **Attachment 10.**

21.3.1.2. Perform an inventory each day the container is opened just prior to final closing. For consecutive shifts within the same day, inventory all material at the end of each shift in which the safe was opened. As a minimum, conduct inventories of controlled components at least once each month, or when directed by CONAUTH.

21.3.1.2.1. Two properly trained and authorized individuals must conduct and document all inventories of controlled components. Both individuals will verify all information directly off of the material against the appropriate USAFE Form 31 entry.

21.3.1.3. If the components are contained within an original sealed kit or box, the kit/box nomenclature, part number and serial number will be documented on the USAFE Form 31 and used for accountability purposes. It is not necessary to open a sealed box or kit just to get the information off the components inside for accountability purposes. If not within a sealed box or kit, enter the information off each item on the inventory form. If a sealed box is opened for any reason, the required information for each of the components contained within must be entered on the inventory form before the safe drawer is closed.

21.3.1.3.1. National Security Agency (NSA) supplied tamper-indicating bags may be used to store controlled components. The bags are serial numbered controlled and provide readily visible indications of opening or tampering.

21.3.1.3.2. Prior to placing controlled components inside the bag a normal physical inventory of all the material must be performed and documented. Once inside the sealed tamper-indicating bag, the inventory may be performed by verifying the bags serial number so long as there is no evidence of tampering. There is no requirement to periodically open a properly documented NSA bag for inspection if it shows no signs of tampering.

21.3.1.4. When a component is permanently installed, destroyed or transferred to another location, it can be removed from the existing USAFE Form 31.

21.3.1.5. USAFE Form 31 is intended to be used until completely full. Once full, keep for 6 months plus the current record.

21.3.2. Use USAFE Form 39, *Weapons Storage and Security system (WS3) Controlled Component Issuing Log*, to document the issue, receipt, turn-in, installation, and destruction of controlled components.

21.3.2.1. Procedures for completing USAFE Form 39s are contained in **Attachment 9.**

21.3.2.2. Keep completed form for 6 months plus the current record.

21.3.3. Once a component is permanently installed in a WSV, RMF/LMF, etc., enter its nomenclature and serial numbers into Integrated Maintenance Data System (IMDS) automated history for the WSV or LMF/RMF.

21.3.4. Controlled components (e.g., AU, VP, etc.) issued from FSP and installed will be documented in IMDS and annotated in the IMDS automated history for the location, such as LMF, RMF, Protected Aircraft Shelter (PAS) or WSV.

21.3.5. While not controlled components; compact flash cards used to transfer data from the MP will be identified and used only for this purpose. Units are authorized to commercially procure as many cards as necessary to meet local requirements. Control in accordance with **Attachment 3**.

21.4. **Controlled Component Destruction**. Destroy compromised or defective EPROMs in accordance with T.O. 11N-50-1003, 11N-50-1003-1, and/or 11N-50-1004.

21.4.1. When MPHDs are deemed defective or compromised, send a request for disposition to the applicable addresses listed in **Attachment 5**. All MPHDs must be controlled according to this instruction until returned to AFNWC/NCSW/OL-SA for destruction.

21.5. **Controlled Component Requisition & Receipt**. EPROMS and MPHDs are not FSP items; base supply will not procure, issue, or stock. Order these through the CONAUTH.

21.5.1. **User Procedures.**

21.5.1.1. Units must submit a consolidated message via a Field Assistance Request (FAR) for quantities of EPROM/MPHDs required in the next shipment.

21.5.2.1. Submit requests immediately when the quantity of on-hand spare EPROMs reaches two or spare MPHDs reaches four.

21.5.2.2. **CONAUTH Procedures.** Resolve emergency requests from the unit by transferring stocks within theater and/or CONAUTH request for emergency restock from AFNWC/NCSW/OL-SA.

21.5.3. **Controlled Component Receipt Procedures.** The account manager will receive EPROMs and MPHDs from DCS. Two personnel from the COMSEC account must receive the shipment due to the special handling of "**TWO SIGNATURES REQUIRED**" for these items. The account manager will transport and store EPROMs and MPHDs under Two-Person Concept.

21.5.3.1. Do not enter EPROMS or MPHDs into the COMSEC Material Control System. Do not voucher the documentation received with the EPROMs and MPHDs or send to the central office of record (COR).

21.5.3.2. The account manager will acknowledge receipt of the EPROMs and MPHDs as listed on the AF Form 310 included in the package received from DCS. Two COMSEC account personnel must verify the material received by serial number, sign the receipt, and mail it back to AFNWC/NCSW/OL-SA, 230 Hall Blvd Suite 224, San Antonio TX 78243-7056.

21.5.3.3. Transfer EPROMs and MPHDs from COMSEC accounts to the communications or WSV maintenance section within 72 hours of receipt.

21.5.3.4. When receipted by the communications or WSV maintenance section, the packaged EPROM kit or MPHD will be immediately removed from all packaging and added to appropriate inventory sheet in accordance with paragraph **21.5** It is not necessary to unseal and open the kit/box itself unless it shows signs of tampering. Kits/boxes that remain sealed can be tracked on the inventory forms by the kit/box information.

21.5.3.5. If the box seal is damaged or shows signs of tampering, or as otherwise necessary when the box is opened, conduct an inspection of each individual EPROM or the MPHD for evidence of tampering or damage. Once inspected, return any components to their packaging/ box/kit to prevent damage while in storage.

JOHN K. MCMULLEN, Major General, USAF
Director of Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoD 5200.1-V1, *DoD Information Security Program: Overview, Classification and Declassification,* 24 February 2012

DoDS-5210.41-M/AFMAN 31-108 V1, (S) *The Nuclear Weapon Security Manual* (U), 1 February 2010

DoDM5210.42_AFMAN13-5011, *Nuclear Weapons Personnel Reliability Program (PRP),* 29 May 2015

AFI 16-1404, *Air Force*ictect*Information Security Program*, 29 May 2015

AFI 21-200, *Munitions and Missile Maintenance Management* and the USAFE Supplement, 02 January 2014

AFI 21-203, *Nuclear Accountability Procedures,* 12 May 2016

AFPD 17-1, *Information Dominance Governance and Management*, 12 April 2016

AFMAN 33-283, *Communications Security (COMSEC) Operations* (FOUO), 3 September 2014

AFI 33-360, *Publications and Forms Management*, 1 December 2015

AFMAN 33-363, *Management of Records*, 1 March 2008

AFI 91-104, *Nuclear Surety Tamper Control and Detection Programs*, 23 April 2013

T.O. 11N-50-1003-1, *Console Group OJ-619/FSQ-143(V) and Monitor-Indicator Group OD-203/ FSQ-143(V) Weapons Storage and Security System AN/FSQ-143(V)*

T.O. 11N-50-1004, *Processor, Vault Control Group OL-398/FSQ-143(V) Weapons Storage and Security System AN/FSQ-143(V)*

T.O. 11N-50-1005, *Coder-Transfer Group OX-69/FSQ-143(V) Weapons Storage and Security System AN/ FSQ-143(V)*

T.O. 11N-50-1006, *Depot Overhaul Instructions With Illustrated Parts Breakdown, Vault Cover Plate Assembly and Vault Screw Assembly; Processor, Vault Control Group OL-398/FSQ-143(V); Weapons Storage and Security System AN/FSQ-143(V)*

T.O. 11N-50-1008, *Deactivation and Reactivation Instructions, Weapons Storage and Security System AN/FSQ-143(V)*

AFKAG-2L, *Air Force COMSEC Accounting Manual*, 15 May 2007

DCS 5200.2-M, *Defense Customer Service Guide*

ACO Directive 80-6/ECI 6801.01, *Nuclear Surety Management for the WS3*, 9 December 2015

Prescribed Forms

USAFE Form 31, *Weapons Storage and Security System (WS3) Controlled Component Inventory*

USAFE Form 39, *Weapons Storage and Security System (WS3) Controlled Component Issuing Log*

USAFE Form 701, *Weapons Storage and Security System (WS3) COMSEC Inventory*

USAFE Form 702, *Weapons Storage and Security System (WS3) COMSEC Module Issuing Log*
USAFE Form 703, *Weapons Storage and Security System (WS3) COMSEC Maintenance Code Tracking*

USAFE Form 704, *Weapons Storage and Security System (WS3) COMSEC Mass Code Tracking*

Adopted Forms

DD Form 1387, *Military Shipment Label*

DD Form 1384, *Transportation Control and Movement Document*

SF Form 153, *COMSEC Material Report*

SF Form 700, *Security Container Information*

SF Form 702, *Security Container Check Sheet*

AF Form 310, *Document Receipt and Destruction Certificate*

AF Form 847, *Recommendation for Change of Publication*

AF Form 1109, *Visitor Register Log*

DCS Form 1, *Receipt to Sender*

DCS Form 10-R, *Defense Courier Service Authorization Record*

Abbreviations and Acronyms

AAAL—Access Authority Authentication List

AC—Alternating Current

AD—Allied Command Operations Directive

ALC—Accounting Legend Code

AFNWC/NCSW/OL—SA - Air Force Nuclear Weapons Center, Nuclear Systems Division, WS3 Branch, Operating Location San Antonio

AU—Authentication Unit

CAP—Cryptographic Access Program

COMSEC—Communications Security

CONAUTH—Controlling Authority

COR—Central Office of Record

CRO—COMSEC Responsible Officer

CSM—Code Storage Module

CTG—Code Transfer Group

CTU—Code Transfer Unit

DA—Data Authenticator

DCS—Defense Courier Service

DIRNSA—Director, National Security Agency

DTRA—Defense Threat Reduction Agency

EAL—Entry Authority List

EAP—Emergency Action Plan

EE—Emergency Evaluation

EPROM—Erasable Programmable Read-Only Memory

FAR—Field Assistance Request

FOUO—For Official Use Only

FSP—Forward Supply Point

GSA—General Services Administration

HAF—Headquarter Air Force

HN—Host Nation

ID—Identification

IMDS—Integrated Maintenance Data System

LMF—Local Monitoring Facility

MAJCOM—Major Command

MASO—Munitions Accountability Systems Officer

MFR—Memorandum for Record

MP—Message Processor

MPHD—Message Processor Hard Drive

NOFORN—Not Releasable to Foreign Nationals

NSA—National Security Agency

OI—Operating Instruction

PDS—Practice Dangerous to Security

PRP—Personnel Reliability Program

RMF—Remote Monitoring Facility

S/N—Serial Number

SCP—Shelter Control Panel

SF—Standard Form

TCN—Transportation Control Number

TD—Time Delay

TDY—Temporary Duty

T.O—Technical Order

TPC—Two Person Control

URC—Universal Release Code

US—United States

VP—Vault Processor

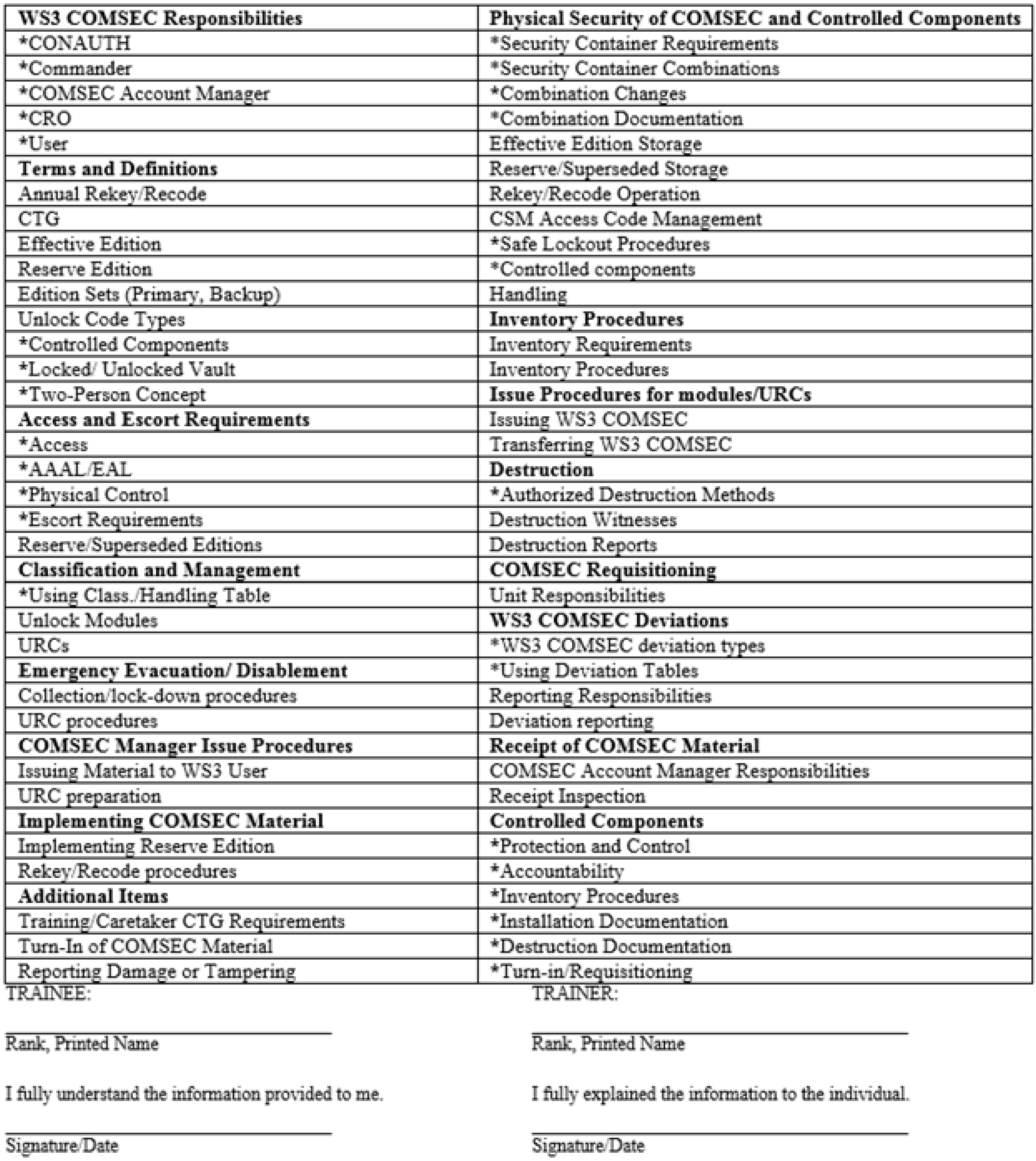
WS3—Weapon Storage and Security System

WSV—Weapons Storage Vault

Attachment 2

WS3 COMSEC TRAINING

A2.1. WS3 COMSEC Training Form. Personnel with access to controlled components (e.g., WS3 Communications personnel) require training on only those tasks identified with an "*". Personnel with access to trackable WS3 COMSEC will be trained on all tasks.



WS3 COMSEC Responsibilities	**Physical Security of COMSEC and Controlled Components**
*CONAUTH	*Security Container Requirements
*Commander	*Security Container Combinations
*COMSEC Account Manager	*Combination Changes
*CRO	*Combination Documentation
*User	Effective Edition Storage
Terms and Definitions	Reserve/Superseded Storage
Annual Rekey/Recode	Rekey/Recode Operation
CTG	CSM Access Code Management
Effective Edition	*Safe Lockout Procedures
Reserve Edition	*Controlled components
Edition Sets (Primary, Backup)	Handling
Unlock Code Types	**Inventory Procedures**
*Controlled Components	Inventory Requirements
*Locked/ Unlocked Vault	Inventory Procedures
*Two-Person Concept	**Issue Procedures for modules/URCs**
Access and Escort Requirements	Issuing WS3 COMSEC
*Access	Transferring WS3 COMSEC
*AAAL/EAL	**Destruction**
*Physical Control	*Authorized Destruction Methods
*Escort Requirements	Destruction Witnesses
Reserve/Superseded Editions	Destruction Reports
Classification and Management	**COMSEC Requisitioning**
*Using Class./Handling Table	Unit Responsibilities
Unlock Modules	**WS3 COMSEC Deviations**
URCs	*WS3 COMSEC deviation types
Emergency Evacuation/ Disablement	*Using Deviation Tables
Collection/lock-down procedures	Reporting Responsibilities
URC procedures	Deviation reporting
COMSEC Manager Issue Procedures	**Receipt of COMSEC Material**
Issuing Material to WS3 User	COMSEC Account Manager Responsibilities
URC preparation	Receipt Inspection
Implementing COMSEC Material	**Controlled Components**
Implementing Reserve Edition	*Protection and Control
Rekey/Recode procedures	*Accountability
Additional Items	*Inventory Procedures
Training/Caretaker CTG Requirements	*Installation Documentation
Turn-In of COMSEC Material	*Destruction Documentation
Reporting Damage or Tampering	*Turn-in/Requisitioning

TRAINEE:

____
Rank, Printed Name

I fully understand the information provided to me.

____
Signature/Date

TRAINER:

____
Rank, Printed Name

I fully explained the information to the individual.

____
Signature/Date

Attachment 3

WS3 COMSEC AND CONTROLLED COMPONENTS CLASSIFICATION AND HANDLING

Table A3.1. WS3 COMSEC and Controlled Components Classification and Handling.

Component	Highest Classification	Two-Person Concept	Special Handling Instructions
Rekey Module	SECRET CRYPTO NOFORN	No	1,2,5
Recode Module	SECRET NOFORN	No	1,2,5
CSM	SECRET NOFORN	No	1,2,5 Protect CSM Access Codes for Effective edition material (once changed from the shipping code)
URC	SECRET NOFORN	No	1,2,5 Effective edition "A" and "B" URCs will never be stored together in the same facility.
Unlock Module	SECRET NOFORN	No	1,2,3,5 Classify unlock modules SECRET - NOFORN after loading them with any code from the CSM or URC cards. Unlock modules remain classified SECRET - NOFORN until the issuing agency verifies all loaded codes have been erased. Unlock modules that have been erased (do not contain any codes) are not COMSEC material and are unclassified.
CTU	UNCLASS	No	3
Unlocked safe Drawer containing Effective edition CTG	SECRET CRYPTO NOFORN	Yes	5 Two-Person requirement is based on the necessity to prevent a lone individual from having access to both "A" and "B" material. Following issue, the individuals accepting responsibility for the modules and/or URCs are not required to remain together.
Locked Vault	UNCLASS	No	Requirements in paragraph 3.7 met.

Component	**Highest Classification**	**Two-Person Concept**	**Special Handling Instructions**
Unlocked Vault	SECRET CRYPTO NOFORN	Yes	Requirements in paragraph 3.10 apply.
Vault Processor	SECRET NOFORN	Yes	1,2 The VP is unclassified however; it becomes a controlled component once GOLD EPROMs are installed. It is classified SECRET (NOFORN) when loaded with operational codes. If VP is compromised, the operational codes which reside in IC U18 are also compromised; a system wide rekey/recode must be accomplished. The VP becomes unclassified after performance of procedures in T.O. 11N-50-1004 to remove IC U18 and/or when the operational codes superseded; however it still requires control under Two-Person Concept to prevent unauthorized tampering until the GOLD EPROM is removed.
Authentication Unit	SECRET CRYPTO NOFORN	Yes	1,2 The AU is unclassified. It becomes a controlled component once GOLD EPROMs are installed. It is classified SECRET CRYPTO (NOFORN) when loaded with operational keys. It becomes unclassified in the event of a power loss; however it still requires control under Two-Person Concept to prevent unauthorized tampering until the GOLD EPROMs are removed.
GOLD EPROM	SECRET CRYPTO NOFORN	Yes	1,2 EPROMs have the same classification as the information which is loaded into them. Surplus GOLD EPROMs require the same level of protection as those operationally configured within WSVs.
BRONZE EPROM	UNCLASS	No	Never install any component equipped with BRONZE EPROMs into an operational system.

Component	Highest Classification	Two-Person Concept	Special Handling Instructions
Message Processor (MP)	UNCLASS	Yes	1,2 The MP is not a controlled component until the Message Processor Hard Drive is installed.
Message Processor Hard Drive (MPHD)	UNCLASS	Yes	1,2 The MPHD is unclassified; however it requires constant protection from access by a lone or unauthorized individual. Never install a defective or compromised MPHD into an MP. If an MPHD is defective or compromised, it is no longer controlled under the Two-Person Concept and can be returned to the Depot via U.S. Registered Mail.
Data Authenticator (DA)	SECRET CRYPTO NOFORN	Yes	1,2 The DA is unclassified. It becomes a controlled component once GOLD EPROMs are installed. It is classified SECRET CRYPTO (NOFORN) when loaded with operational keys. It becomes unclassified in the event of a power loss; however it still requires control under Two-Person Concept to prevent unauthorized tampering when the GOLD EPROM is installed.
AU-VP Cable	UNCLASS	Yes	4
K1, K2, K3 relays	UNCLASS	Yes	4
Alternate Operating System Time Delay	UNCLASS	Yes	4
Training/Caretaker CTG Material	UNCLASS NOFORN	No	3
Compact Flash Cards	UCNI	No	3 Events Files, Site Unique Configuration or any other information downloaded from the Message Processor will be controlled as UCNI information.
Reversing Contact Starter	UNCLASS	Yes	4
Notes: 1. Each person issued a module or URC card or Controlled Component is responsible for			

<table>
<tr><th>Component</th><th>Highest Classification</th><th>Two-Person Concept</th><th>Special Handling Instructions</th></tr>
<tr><td colspan="4">its control until returning it to the issuing office, properly transferring it to another authorized person or installing/destroying it.
2. Do not carry modules of any type, URCs, or Controlled Components into public areas including dining facilities, finance centers, base exchanges, military personnel flights, etc.
3. Control in a manner to prevent misuse, theft, sabotage, and/or tampering.
4. Becomes a controlled component following two-person inspection and installation in an operational WSV.
5. Designated “A” and “B” personnel will handle the corresponding material.</td></tr>
</table>

Attachment 4

WS3 COMSEC INCIDENTS

Table A4.1. (FOUO) Reporting a WS3 COMSEC Practice Dangerous to Security.

Rule	If the PDS Involves:	The COMSEC Account Manager:
1	A. Supersession of Effective edition WS3 COMSEC material outside of anniversary month unless directed by CONAUTH or this instruction. B. Access to WS3 COMSEC material and/or controlled components by a Two-Person Concept team comprised of two individuals who are PRP Interim certified. C. An entry is omitted on WS3 COMSEC Forms (excluding USAFE forms 701/31, see table A4.2, rule 9) but 100 percent control of material maintained.	Send a PDS reports to the CONAUTH within 3 duty days of discovery using addresses in **Attachment 5**. Completes any actions requested by the CONAUTH.
2[1]	A. All other administrative/documentation errors on the WS3 COMSEC forms with 100 percent control of material maintained. B. Destruction of URCs not performed within required time limits, but the material was otherwise properly handled and destroyed.	Does not up channel the PDS. Resolves the situation locally to include notifying the violating unit Commander.
[1] When units resolve the situation locally, a PDS report will still be generated and filed.		

Table A4.2. (FOUO) Reporting a WS3 COMSEC Incident.

Rule	Physical Incidents Include:	The COMSEC Account Manager:
1	A. Unauthorized access to WS3 COMSEC material and/or controlled components to include: 1. Safes containing WS3 COMSEC material and/or controlled components, which are left unsecured or unauthorized personnel have knowledge of safe combination. 2. WS3 COMSEC material and/or controlled components lost or temporarily out of control. 3. Unlocked WSV containing controlled components not attended by an authorized Two-Person Concept team B. An individual has unauthorized access to, or knowledge of, CSM access codes.	Send a physical incident reports to the CONAUTH within 24 hours of discovery using addresses in **Attachment 5**. Completes any actions requested by the CONAUTH

	C. Failure to have an “A” and “B” lock present whenever security containers containing Effective edition WS3 COMSEC material is accessed. D. Access to WS3 COMSEC material by personnel who are PRP suspended or decertified. E. Other US/Host Nation personnel are part of a WS3 Two-Person Concept team performing maintenance on the vault, procedures handling WS3 keyed/ coded material, or handling Two-Person Concept controlled components.	
2	A. An Effective edition URC is inadvertently opened and/or compromised. B. A base-wide rekey/recode is not initiated immediately after an Effective edition URC is inadvertently opened and/or compromised.	
3	A. Destruction of WS3 COMSEC material, MPHDs, GOLD EPROMs or components containing GOLD EPROMs by other than authorized means, such as: 1. Destruction of URCs without required documentation. 2. Destruction of URCs in unauthorized destruction device. 3. Local destruction of any WS3 COMSEC other than URCs. 4. Destruction of GOLD EPROMs not IAW T.O. 11N-50-1003, T.O. 11N-50-1003-1, or T.O. 11N-50-1004. 5. A URC found not completely destroyed in an authorized device.	
4	Known or suspected deliberate falsification or unauthorized re-accomplishment or correction of WS3 COMSEC and/or controlled component documentation (to include using white-out/correction fluid/ correction tape, or erasures).	
5	Unauthorized absences of personnel with access to WS3 COMSEC and/or controlled component.	
6	Installation of any component containing BRONZE EPROMs into an operational WS3 system.	
7	A WS3 COMSEC and/or controlled component is issued to unauthorized individuals.	
8	Using WS3 COMSEC material that is compromised, superseded, defective or previously used (and not authorized for reuse).	
9	Any other incident that may jeopardize the physical security of WS3 COMSEC and/or controlled component. (For Example) Missing required COMSEC accountability records (i.e. USAFE Form 701/702, Destruction Report (SF-153), and Audit Data). Failing to perform an inventory when required.	

10	A. Known or suspected tampering with, or unauthorized modification of, or maintenance on, any WS3 COMSEC material to include Rekey, Recode, CSM, URCs, controlled components, or Unlock modules which are loaded with unlock codes. B. Discovery of a clandestine electronic surveillance or recording device in or near a WS3 COMSEC facility (building in which WS3 COMSEC is used or stored). C. Known or suspected tampering with or unauthorized maintenance on any GOLD EPROM or controlled component installed in a WS3 system. D. Known or suspected tampering with, or unauthorized modification or maintenance on any controlled component discovered during Two-Person recovery procedures IAW T.O. 11N-50-1004.	Send a physical incident reports to the CONAUTH within 24 hours of discovery using addresses in **Attachment 5**. Notify CONAUTH immediately by any available means. Completes any actions requested by the CONAUTH

Attachment 5

WS3 COMSEC MESSAGE ADDRESSES

Table A5.1. WS3 COMSEC Message Addresses.

Reason for Report	Send Action Email to:	Send Information Copy to:	From
Exceptions to provisions of USAFEI 33-283	HQ USAFE/A10NM	HQ USAFE/A10NP	COMSEC Account Manager
Rejectable damage or malfunctions to WS3 COMSEC and/or controlled component	HQ USAFE/A10NM	HQ AFNIC/ECAP DIRNSA/I313/I3171/ I2N HQ USAFE/A10NP AFNWC/NCSW/OL-SA	COMSEC Account Manager
Reportable COMSEC PDS Report	HQ USAFE/A10NM	HQ USAFE/A10NP	COMSEC Account Manager
COMSEC Incident Report	HQ USAFE/A10NM	HQAFNIC/ECAP DIRNSA/I313/I3171/ I2N Violating Unit's Commander HQ USAFE/A10NP	COMSEC Account Manager
CONAUTH Message Requesting WS3 COMSEC material	DIRNSA/Y51/Y17 1	None	HQ USAFE/ A10NM
Unit Message for Implementation of Reserve Material	HQ USAFE/A10NM		COMSEC Account Manager
Request for disposition for superseded/excess WS3 COMSEC material	HQ USAFE/A10NM	HQ USAFE/A10NP	COMSEC Account Manager
Notification that new Reserve edition is received	HQ USAFE/A10NM	HQ USAFE/A10NP	COMSEC Account Manager
CONAUTH disposition message	Applicable COMSEC Account	DIRNSA/I2N/I313/ I3171	HQ USAFE/ A10NM

for superseded/ compromised material		HQ USAFE/A10NP AFNWC/NCSW/OL-SA	
Request for new EPROM/MPHDs	Submit Field Assistance Request (FAR) via NMC2 SharePoint	Send Info e-mail alerting CONAUTH of FAR submission to: HQ USAFE/A10NM	COMSEC Responsible Officer
Notification of defective/compromised MPHD and/or EPROM	Submit Field Assistance Request (FAR) via NMC2 SharePoint	Send Info e-mail alerting CONAUTH of FAR submission to: HQ USAFE/A10NM	COMSEC Responsible Officer

Attachment 6

PROCEDURES TO COMPLETE THE CSM ACCESS CODE SF FORM 700

A6.1. Use the following procedures to record and store CSM access codes on a SF 700, *Security Container Information Form (note: these procedures are meant to be referenced, and are not "steps" required to be checked off).*:

A6.1.1. **Complete Part 1**.

A6.1.1.1. Block 1-3 not required.

A6.1.1.2. Block 4 enter location part 2 will be stored.

A6.1.1.3. Block 5 enter container part 2 will be stored in.

A6.1.1.4. Block 6 enter "CSM".

A6.1.1.5. Block 8 enter "A lock" or "B lock".

A6.1.1.6. Block 9 enter date the CSM code was changed.

A6.1.1.7. Block 10 enter your name and signature (or individual making the change).

A6.1.1.8. Block 11 Enter at least 2 authorized individual's information.

A6.1.2. **On the detachable portion (Part 2A):**

A6.1.2.1. Enter "CSM access code ("Primary" or "Backup") A" or "CSM access code ("Primary" or "Backup") B" (as applicable) in the "Container Number" block.

A6.1.2.2. Enter the CSM access code in the "Combination" Block.

A6.1.2.3. On the back of the form, annotate the edition and register number. Do not annotate the short-title.

A6.1.2.4. Mark the classification "SECRET//NOFORN".

A6.1.3. Place the form inside of the envelope (Part 2) and seal it.

A6.1.4. **On the exterior of the envelope (Part 2):** Ensure all information from part 1 transferred to part 2 if not, fill out part 2 using paragraph A7.1.1.

A6.1.4.1. Mark the front and back, top and bottom of the SF 700 with an overall classification of SECRET//NOFORN.

Attachment 7

PROCEDURES TO COMPLETE THE USAFE FORM 702

A7.1. Use the following procedures to document WS3 COMSEC issue, turn-in, transfer and destruction actions on the USAFE Form 702. (note: these procedures are meant to be referenced, and are not "steps" required to be checked off).

A7.1.1. A separate line entry will be filled out for each module/URC.

A7.2. Issue/Turn-In Procedures.

A7.2.1. Enter the following in the SERIAL NUMBER block (a):

A7.2.1.1. Check either the "A" or "B" block for the module/URC.

A7.2.1.2. Enter S/N for a module or Edition or Reg # for a URC.

A7.2.2. Enter the following in the TYPE CODE block (b):

A7.2.2.1. Check appropriate block for the type of code that is loaded in the module.

A7.2.2.1.1. The Other free text block and space provided is for other types/information (e.g. transfer).

A7.2.3. Enter the following in the VAULT ID NUMBER block (c):

A7.2.3.1. If a Maintenance Code was loaded, enter each vault ID which is loaded in the module.

A7.2.3.2. No entries are required for URC or Mass codes, Rekey or Recode modules, CSMs or URC cards.

A7.2.4. Enter the following in the DATE/TIME OUT block (d):

A7.2.4.1. Annotate Date and Time the module/URC was signed out.

A7.2.5. Enter the following in the FIRST INITIAL, LAST NAME/SIGNATURE block (e):

A7.2.5.1. Annotate printed first initial and full last name and then payroll signature of individual who signs out the module/URC.

A7.2.6. Enter the following in the ISSUED BY NAME/INITIALS block (f):

A7.2.6.1. Annotate printed full last name and initials of individual who authorized the issuing of the module/URC.

A7.2.7. Enter the following in the ACTION TAKEN block (g):

A7.2.7.1. Check appropriate block(s) to show final actions taken with the module/URC.

A7.2.7.1.1. Turned In if it was returned to the storage location.

A7.2.7.1.2. Transferred if it was transferred.

A7.2.7.1.3. Erased when the Unlock Module is erased.

A7.2.7.1.4. Destroyed if the URC was destroyed when authorized.

A7.2.8. Enter the following in the DATE/TIME IN block (h):

A7.2.8.1. Annotate Date and Time the action indicated in block (g) was taken.

A7.2.9. Enter the following in the FIRST INITIAL, LAST NAME/SIGNATURE block (i):

A7.2.9.1. Annotate printed first initial and full last name and then payroll signature of individual who signs in/transfers/destroys the module/URC.

A7.3. Transfer Procedures.

A7.3.1. In the original line entry complete the information for the individual who originally signed out the module/URC.

A7.3.1.1. Check Transferred in the ACTION TAKEN block (g).

A7.3.1.2. Enter the following in the DATE / TIME IN block (h).

A7.3.1.2.1. Annotate Date and Time the module/URC was transferred.

A7.3.1.3. Enter the following in the FIRST INITIAL, LAST NAME / SIGNATURE block (i):

A7.3.1.3.1. Annotate the printed first initial and full last name then payroll signature of the individual who is transferring the module/URC. If that individual is not present to sign at the time of transfer, their payroll signature will be entered upon return.

A7.3.2. Enter the information for the individual who is receiving the module/URC on a new line as follows:

A7.3.2.1. Enter the following in the SERIAL NUMBER block (a):

A7.3.2.1.1. Check either the “A” or “B” block for the module/URC to be transferred.

A7.3.2.1.2. Enter S/N for a module or Edition and Reg # for a URC.

A7.3.2.2. Enter the following in the TYPE CODE block (b):

A7.3.2.2.1. Check appropriate type of code for the transferred module/URC.

A7.3.2.2.1.1. Check the free text block and annotate “Transferred” in the space provided.

A7.3.2.3. Enter the following in the VAULT ID NUMBER block (c):

A7.3.2.3.1. Enter the vault ID’s for the transferred unlock module, otherwise leave blank.

A7.3.2.4. Enter the following in the DATE/TIME OUT block (d):

A7.3.2.4.1. Annotate Date and Time the module/URC was transferred.

A7.3.2.5. Enter the following in the FIRST INITIAL, LAST NAME/SIGNATURE block (e).

A7.3.2.5.1. Annotate the printed first initial and full last name then payroll signature of the individual who is receiving the module/URC. If that individual is not present to sign at the time of transfer, their payroll signature will be entered upon return.

A7.3.2.6. Enter the following in the ISSUED BY NAME/INITIALS block (f):

A7.3.2.6.1. Annotate printed full last name and initials of individual who authorized the transferring of the module/URC .

A7.3.2.7. Enter the following in the ACTION TAKEN block (g).

A7.3.2.7.1. Check appropriate block(s) to show final action taken with the transferred module/ URC.

A7.3.2.7.1.1. Turned In if it was returned to the storage location.

A7.3.2.7.1.2. Transferred if it was again transferred to another individual.

A7.3.2.7.1.3. Erased when the Unlock Module is erased.

A7.3.2.7.1.4. Destroyed if the URC was destroyed.

A7.3.2.7.2. Enter the following in the DATE/TIME IN block (h):

A7.3.2.7.2.1. Annotate Date and Time the action indicated in block (g) was taken.

A7.3.2.7.3. Enter the following in the FIRST INITIAL, LAST NAME/SIGNATURE block (i):

A7.3.2.7.3.1. Annotate printed first initial and full last name and then payroll signature of individual who signs in/transfers/destroys the module/URC.

A7.4. Error Correction.

A7.4.1. In the event a correction is necessary, do not use correction fluid, correction tape, or erasures on the form. Any errors or discrepancies made on the form will be documented as a memorandum for record (MFR) on the reverse of the form. As required, place a single line through the erroneous entry and number the error in the margin clearly corresponding to the error/discrepancy with an “MFR #”. MFRs will be sequentially numbered per form.

A7.4.1.1. Both individuals discovering the error will annotate a brief, dated MFR with their initials on the reverse of the form (e.g., DD MMM YY – DATE INCORRECTLY ENTERED CAUGHT AND CORRECTED ON THE SPOT INITS/INITS).

Attachment 8

PROCEDURES TO COMPLETE THE USAFE FORM 701

A8.1. Use the following procedures to complete and document WS3 COMSEC inventories on the USAFE Form 701. (note: these procedures are meant to be referenced, and are not “steps” required to be checked off).

A8.1.1. Use black or blue ink when making entries on the inventory. Same color must be used throughout the entire form. The current inventory form(s) will be stored within the safe drawer with the material it applies to.

A8.1.2. Annotate **Short Title** (a), **Edition** (b), **Registration #** (c), and **Qty** (d) for each item. Document item serial numbers for COMSEC loaded unlock modules.

A8.1.3. Annotate the “**Page__ of __ Pages**,” “CONTAINER NUMBER” and “MONTH:” blocks.

A8.1.4. Inventories will be documented starting in the left-most open “**INVENTORIES**” block (e) and filling in the next open column to the right for each subsequent inventory. Place an “X” from corner to corner in the block corresponding to each item if it is verified as present.

A8.1.5. Document the date the inventory is performed in the corresponding “**INVENTORY DATES**” block (f).

A8.1.6. Annotate the payroll signature of each individual who performed the inventory in the corresponding “**SIGNATURES OF PERSONS PERFORMING THE INVENTORY**” block (g).

A8.1.7. If multiple inventories are required in one calendar day, simply annotate each additional inventory in the next open column to the right using the same date.

A8.1.8. If more than 39 inventories are performed in one calendar month, the WS3 CRO will initiate a new inventory form and update the “**Page__ of __ Pages**” block.

A8.1.9. When adding new WS3 COMSEC material one individual will annotate IAW paragraph A8.1.1. A second individual will verify the information annotated on the inventory is accurate by checking both the form and the item. Use a specific color when adding items to the inventory. Block the entry up to the date added, date, sign, and explain the reason for the addition (e.g., Received from account, etc.). If a new inventory is printed out, identify items added on the new inventory.

A8.1.10. When deleting material from the inventory, use a specific color different from that used to add material. Block out the remainder of that entry, date, initial, and explain the reason for removal (e.g., Returned to account, Destroyed with voucher number, etc.).

A8.1.11. **Error Correction**

A8.1.11.1. In the event a correction is necessary; do not use correction fluid, correction tape, or erasures on the form. Any errors or discrepancies made on the form will be documented as a MFR on the reverse of the form. As required, place a single line through the erroneous entry and number the error in the margin clearly corresponding to the error/discrepancy with an “MFR #”. MFRs will be sequentially numbered per form.

A8.1.11.2. Both individuals discovering the error will annotate a brief, dated MFR with their initials on the reverse of the form (e.g., DD MMM YY – SHORT-TITLE INCORRECTLY ENTERED CAUGHT AND CORRECTED ON THE SPOT INITS/INITS).

A8.1.12. Each form will be closed out the following month during the first safe opening by placing a vertical line along with the statement “Inventory Closed” through the first open INVENTORIES column immediately adjacent to the last documented inventory. Annotate the signature and date of the individual closing out the form in that column. Only one signature is required.

A8.1.13. The WS3 CRO will review completed forms for errors within 20 duty days of closing the form. This review will include both a review of the inventory form for any errors, and a comparison of the form against other accountability documents (e.g. USAFE Form 702 and SF Form 702) for that period to ensure no inventories were missed or improperly documented. Once the review is complete and any deficiencies noted are documented, investigated, and reported as necessary, the WS3 CRO will date and sign the MONTHLY REVIEW block (h).

Attachment 9

PROCEDURES TO COMPLETE THE USAFE FORM 39

A9.1. Use the following procedures to document WS3 Controlled Components issue, turn-in installation, destruction, and transfer actions on the USAFE Form 39. (note: these procedures are meant to be referenced, and are not "steps" required to be checked off).

A9.1.1. Enter the following in the SERIAL NUMBER block (a):

A9.1.1.1. Enter the S/N of the Kit/Box/Component.

A9.1.2. Enter the following in the ITEM TYPE block (b):

A9.1.2.1. Check appropriate block for type of component.

A9.1.2.2. The Other free text block and space provided is for other types/information (e.g. transfer).

A9.1.3. In the DATE/TIME OUT block (c) annotate the Date and Time the component was signed out to each individual.

A9.1.4. Enter the following in the FIRST INITIAL LAST NAME & SIGNATURES block (d):

A9.1.4.1. In the top two blocks, annotate printed first initial and full last name and payroll signature of the authorized "A" lock who signed out the component.

A9.1.4.2. In the bottom two blocks, annotate printed first initial and full last name and payroll signature of the authorized "B" lock who signed out the component.

A9.1.5. Enter the following in the ACTION TAKEN block (e):

A9.1.5.1. Check appropriate block or fill in the blank to show the final action taken with the component.

A9.1.5.2. More than one block may be checked depending on actions taken with the component.

A9.1.5.2.1. Check Installed in if it was installed in a vault or either monitoring facility.

A9.1.5.2.1.1. If it was installed in a vault, enter the vault ID in the blank.

A9.1.5.2.1.2. If it was installed in either the LMF or RMF, check the applicable location.

A9.1.5.2.2. Check Transferred if it was transferred to another authorized individual

A9.1.5.2.3. Check Returned if it was returned to the storage location.

A9.1.5.2.4. Check Destroyed if the component was destroyed when authorized.

A9.1.6. In the DATE/TIME IN block (f) annotate the Date and Time the component was returned/installed in/destroyed.

A9.1.7. Enter the following in the FIRST INITIAL, LAST NAME & SIGNATURES block (g):

A9.1.7.1. In the top two blocks, annotate printed first initial and full last name and payroll signature of the authorized “A” lock who signed in the component.

A9.1.7.2. In the bottom two blocks, annotate printed first initial and full last name and payroll signature of the authorized “B” lock who signed in the component.

A9.2. Component Transfer Procedures

A9.2.1. In the original line entry, complete the information for the individuals who originally signed out the component.

A9.2.1.1. Check Transferred in the ACTION TAKEN block (e):

A9.2.1.2. In the DATE/TIME IN block (f) annotate the Date and Time the component was transferred to each individual.

A9.2.1.3. Enter the following in the FIRST INITIAL LAST NAME & SIGNATURES block (g):

A9.2.1.3.1. In both name blocks annotate the printed first initial and full last name of both individuals who are transferring the component. If those individuals are not present to document the form themselves the individual who authorized the transfer will print the required names.

A9.2.1.3.2. When the personnel who transferred the component return, they will both enter their payroll signatures.

A9.2.2. On a new line enter the information for the individuals who are receiving the component.

A9.2.2.1. Enter the S/N of the component being transferred in the SERIAL NUMBER block (a):

A9.2.2.2. In the ITEM TYPE block (b) check the Other block and annotate “Transferred” in the space provided.

A9.2.2.3. In the DATE/TIME OUT block (c) annotate the Date and Time the component was signed out for each of the individuals.

A9.2.2.4. Enter the following in the FIRST INITIAL LAST NAME & SIGNATURES block (d):

A9.2.2.4.1. Annotate printed first initial and full last names and then payroll signature of both properly authorized individuals who are receiving the transferred component.

A9.2.2.4.2. The individual who authorized the transfer will annotate the printed first initial and full last names of both individuals who are receiving the transferred component if those individuals are not present to sign the form themselves.

A9.2.2.4.3. When the individuals who received the transferred component return, they will annotate their payroll signatures.

A9.2.2.5. Enter the following in the ACTION TAKEN block (e):

A9.2.2.5.1. Check appropriate block or fill in the blank to show final action taken with the component.

A9.2.2.5.2. More than one block may be checked depending on actions taken with the component:

A9.2.2.5.2.1. Check Installed in if it was installed in a vault or either of the monitoring facilities.

A9.2.2.5.2.1.1. If it was installed in a vault, enter the vault ID in the blank.

A9.2.2.5.2.1.2. If it was installed in either the LMF or RMF, check the applicable location.

A9.2.2.5.2.2. Check Transferred if it was again transferred to another authorized individual.

A9.2.2.5.2.3. Check Returned if it was returned to the storage location.

A9.2.2.5.2.4. Check Destroyed if the component was destroyed when authorized.

A9.2.2.6. In the DATE/TIME IN block (f) annotate Date and Time the component was signed in for each individual.

A9.2.2.7. Enter the following in the FIRST INITIAL LAST NAME & SIGNATURES block (g).

A9.2.2.7.1. In the top two blocks, annotate printed first initial and full last name and payroll signature of the authorized "A" lock who signed in the component.

A9.2.2.7.2. In the bottom two blocks, annotate printed first initial and full last name and payroll signature of the authorized "B" lock who signed in the component.

A9.3. Error Correction.

A9.3.1. In the event a correction is necessary; do not use correction fluid, correction tape, or erasures on the form. Any errors or discrepancies made on the form will be documented as a MFR on the reverse of the form. As required, place a single line through the erroneous entry and number the error in the margin clearly corresponding to the error/discrepancy with an "MFR #". MFRs will be sequentially numbered per form.

A9.3.2. Both individuals discovering the error will annotate a brief, dated MFR with their initials on the reverse of the form (e.g., DD MMM YY – SHORT-TITLE INCORRECTLY ENTERED CAUGHT AND CORRECTED ON THE SPOT INITS/INITS)

Attachment 10

PROCEDURES TO COMPLETE THE USAFE FORM 31

A10.1. Use the following procedures to complete and document WS3 Controlled Component inventories on the USAFE Form 31. The current inventory form(s) will be stored within the safe drawer with the material it applies to. (note: these procedures are meant to be referenced, and are not "steps" required to be checked off).

A10.1.1. Annotate NOMENCLATURE (a), VERSION (b), PART NUMBER (c), and SERIAL NUMBER (d) for each individual item. If the items are inside a sealed kit or box, enter the Nomenclature, Version #, Part Number and Serial Number of the kit/box.

A10.1.2. Annotate the "PAGE __ OF __ PAGES," "CONTAINER NUMBER," and "START DATE" blocks.

A10.1.3. Inventories will be documented starting in the left-most open "INVENTORIES" block (e) block and filling in the next open column to the right for each subsequent inventory. Place an "X" from corner to corner in the block corresponding to each item if it is verified as present.

A10.1.4. Document the date the inventory is performed in the corresponding "INVENTORY DATES:" block (f).

A10.1.5. Annotate the payroll signature of each individual who performed the inventory in the corresponding "SIGNATURES OF PERSONS PERFORMING THE INVENTORY" block (g).

A10.1.6. If multiple inventories are required in one calendar day, simply annotate each additional inventory in the next open column to the right using the same date.

A10.1.7. If more than 24 individual components are stored within one container, initiate additional inventory forms and update each of the "PAGE__ OF__ PAGES" blocks on the forms sequentially from 1 up to the number of forms that are in use.

A10.1.8. When adding new controlled components, one individual will annotate the USAFE Form 31 with the required information off the item/kit/box. A second individual will verify the information annotated on the inventory is accurate by checking both the form and the item. Use a specific color when adding items to the inventory. Block the entry up to the date added, date, sign, and explain the reason for the addition (e.g., Received from account, etc.) If a new inventory is printed out, identify items added on the new inventory.

A10.1.9. If a component is permanently installed, destroyed, or transferred, document the removal from the inventory form using a specific color different from that used to add material. Block out the remainder of that entry, date, initial, and explain the reason for removal (e.g., Installed, Destroyed, etc.).

A10.1.10. **Error Correction**.

A10.1.10.1. In the event a correction is necessary, do not use correction fluid, correction tape, or erasures on the form. Any errors or discrepancies made on the form will be documented as a MFR on the reverse of the form. As required, place a single line through the erroneous entry and number the error in the margin clearly corresponding to the error/discrepancy with an “MFR #”. MFRs will be sequentially numbered per form.

A10.1.10.2. Both individuals discovering the error will annotate a brief, dated MFR with their initials on the reverse of the form (e.g., DD MMM YY – EPROM VERSION NUMBER INCORRECTLY ENTERED CAUGHT AND CORRECTED ON THE SPOT INITS/INITS).

A10.1.11. The USAFE Form 31 is not a “monthly” form, each will be used until all the available inventory date blocks are full, at which time the “CLOSE DATE” block will be annotated.

Attachment 11

PROCEDURES TO COMPLETE THE USAFE FORM 703/704

A11.1. Use the following procedures to complete and document maintenance/mass code tracking on the USAFE Form 703/704. (note: these procedures are meant to be referenced, and are not “steps” required to be checked off).

A11.2. Use black or blue ink when making entries on the USAFE form 703/704. Same color ink must be used throughout the entire form.

A11.3. When initiating a new form, enter the COMSEC edition, vault ID number (USAFE Form 704 only), primary A/B CSM serial numbers and backup A/B CSM serial numbers in the appropriate blocks.

A11.4. Expending maintenance or mass code:

A11.4.1. Enter a slash through the number of the code being expended in block (a).

A11.4.2. Enter the date the code was expended in block (b).

A11.4.3. Enter the initials of the first individual who expended the code in block (c).

A11.4.4. Enter the initials of the second individual who expended the code in block (d).

A11.4.4.1. Enter the reason for use of the code (free text) in block (e).

A11.5. CSM Update. For the monthly CSM update, fill out the following information for every code that is being updated.

A11.5.1. Enter the date the CSM update occurred in block (f).

A11.5.2. Enter the initials of the first individual who performed the CSM update in block (g).

A11.5.3. Enter the initials of the second individual who performed the CSM update in block (h).

A11.5.3.1. Enter a slash through the number of the code being updated as expended in block (i).

A11.6. Error Correction.

A11.6.1. In the event a correction is necessary; do not use correction fluid, correction tape, or erasures on the form. Any errors or discrepancies made on the form will be documented as a MFR on the reverse of the form. As required, place a single line through the erroneous entry and number the error in the margin clearly corresponding to the error/discrepancy with an “MFR #”. MFRs will be sequentially numbered per form.

A11.6.2. Both individuals discovering the error will annotate a brief, dated MFR with their initials on the reverse of the form (e.g., DD MMM YY – INCORRECT DATE ENTERED CAUGHT AND CORRECTED ON THE SPOT INITS/INITS).

A11.6.3. The USAFE Form 703/704 is not a “monthly” form, each will be used until all the available codes have been expended or until creation of a new form due to implementation of a new COMSEC edition.